Le droit à l'oubli

Maryline Boizard, Annie Blandin-Obernesser, Cristina Corgas-Bernard, Gilles Dedessus Le Moustier, Sébastien Gambs, Catherine Lejealle, Sylvie Moisdon-Chataigner, Philippe Pierre, Guillaume Piolle, Laurent Rousvoal

LE DROIT A L'OUBLI

Responsable scientifique du projet :

Maryline Boizard

Maître de conférences - HDR

Faculté de droit et de science politique, Rennes 1

Institut de l'Ouest : Droit et Europe

IODE UMR CNRS 6262

Recherche réalisée avec le soutien de la Mission de recherche Droit et Justice

Février 2015

EQUIPE DE CHERCHEURS

- **Maryline Boizard**, Responsable scientifique du projet, Maître de conférences HDR, Droit privé et Sciences criminelles, Faculté de droit et de science politique, Rennes 1, IODE (UMR CNRS 6262), spécialiste de droit de la propriété industrielle et de droit de l'Internet.

- **Annie Blandin**, Professeur, Droit public, Télécom Bretagne, spécialiste du droit de l'informatique et des réseaux.

- **Cristina Corgas-Bernard**, Maître de conférences HDR, Droit privé et Sciences criminelles, Faculté de droit et de science politique, Rennes 1, spécialiste de droit de la responsabilité et droit médical.

- **Gilles Dedessus-le Moustier**, Maître de conférences HDR, Droit privé et Sciences criminelles, Faculté de droit et de science politique, Rennes 1, spécialiste de Droit du travail et des nouvelles technologies.

- **Sébastien Gambs** : Maître de conférences, Informatique, ISTIC, Rennes 1, Chaire de recherche commune avec INRIA, spécialiste en protection de la vie privée.

- **Catherine Lejealle,** Docteur en sociologie et ingénieur Télécom, spécialiste en sociologie des usages des TIC.

- **Sylvie Moisdon-Chataigner**, Maître de conférences HDR, Droit privé et Sciences criminelles, Faculté de Droit et de Science politique, Rennes 1, spécialiste de droit des personnes.

- **Philippe Pierre** : Professeur, Droit privé et sciences criminelles, Faculté de Droit et de Science politique, Rennes 1, spécialiste de la responsabilité et du droit médical.

- **Guillaume Piolle**, Professeur assistant, Informatique, Supélec Rennes, spécialiste de la protection des données personnelles et des systèmes d'informatique juridique.

- **Laurent Rousvoal**, Maître de conférences en droit privé et Sciences criminelles, Faculté de droit et de science politique, Université de Rennes 1, IODE (UMR CNRS 6262), spécialiste de droit pénal.

Stagiaires

- **Amélien Delahaie**, étudiant en droit, Magistère Université de Poitiers.

- **Léa Monel**, étudiante en droit, Magistère Université de Poitiers.

Le présent document constitue le rapport scientifique d'une recherche réalisée avec le soutien du GIP Mission de recherche Droit et justice (convention 11.25). Son contenu n'engage que la responsabilité de ses auteurs.

SOMMAIRE

INTRODUCTION

L'intérêt économique des données concernant chacun d'entre nous n'est plus à démontrer. C'est encore plus vrai à l'ère du numérique et d'Internet où l'on passe à une massification de l'exploitation des données, tout spécialement, des données personnelles. Les enjeux financiers sont colossaux et génèrent nécessairement des conflits car l'exploitation qui est faite de ces données peut heurter les droits fondamentaux de la personne. Dès 1978, le législateur français réagissait en adoptant une loi dite informatique et libertés, destinée à assurer la protection des personnes contre l'exploitation abusive des données à caractère personnel[1]. Il s'agissait de protéger les données à caractère personnel des personnes physiques face aux divers usages de l'informatique. D'autres textes ont suivi, notamment à l'échelon européen. C'est le cas de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995[2]. Au fil des années, a néanmoins émergé une revendication spécifique, celle d'un « droit à l'oubli », qui avec l'arrivée de la digitalisation, s'est finalement étendue à un « droit à l'oubli numérique ». L'apparition de ce nouveau concept nous interroge et a conduit la Mission de recherche Droit et Justice à lancer, au mois de juin 2011, un appel d'offre devant permettre de déterminer le contenu, les limites et les incidences d'un tel concept. Les instances européennes, elles-mêmes, se sont emparées de la question en adoptant, le 25 janvier 2012, une proposition de règlement faisait une référence directe au droit à l'oubli[3], choix sur lequel est néanmoins revenu le Parlement européen[4]. Comment expliquer le recours à un concept qui n'est pas consacré juridiquement ? Doit-on considérer que le droit positif n'offre pas les garanties suffisantes à la préservation des droits et libertés fondamentaux ? Faut-il y voir un concept mou, non juridique ou bien une notion standard qui serait un critère d'appréciation du respect des droits fondamentaux ? Convient-il d'aller encore plus loin en traduisant les demandes d'un droit à l'oubli comme le souhait de voir apparaître sur la scène juridique un nouveau droit autonome ? Pour répondre à ces questions il convient, avant toute chose, de préciser trois notions : l'oubli, l'oubli numérique et le droit à l'oubli.

---

[1] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

[2] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, modifiée par une directive du 12 juillet 2002, elle-même complétée par une directive du 25 novembre 2009.

[3] Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, plus simplement nommé Règlement général sur la protection des données, COM/2012/011 final - 2012/0011 (COD).

[4] Résolution législative du Parlement européen du 12 mars 2014 sur la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)).

La notion d'oubli correspond à deux réalités bien distinctes. D'une part, l'oubli évoque l'échec, la défaillance de la mémoire et revêt alors une coloration négative[5]. Dans ce sens, l'oubli est une faiblesse. Parce qu'il empêche l'individu de se souvenir, il constitue un obstacle à la conservation des connaissances. Plus encore, l'oubli représente un obstacle à l'exercice du devoir de mémoire nécessaire pour ne pas reproduire les erreurs du passé.

Dans les formes les plus sévères, l'oubli est une forme de dégénérescence neurologique. Il résulte de maladies neurodégénératives qui entraînent la perte progressive des fonctions mémorielles (c'est le cas de la maladie d'Alzheimer par exemple). Dans ce cas, oublier « c'est s'approcher de la mort »[6]. Le droit appréhende ce comportement en sanctionnant certains oublis (oublier de remplir sa déclaration d'impôt, oublier de payer son loyer etc…). L'oubli, acte involontaire, peut être préjudiciable à son auteur ou à un tiers. Sauf circonstances exceptionnelles, il est sanctionné lorsqu'il constitue la violation d'une obligation légale ou conventionnelle. Dans cette conception, l'oubli serait en quelque sorte une « mémoire en défaut »[7].

D'autre part, l'oubli c'est la volonté, la faculté d'oublier. Dans cette perspective, l'oubli peut être envisagé de manière positive. C'est la capacité à oublier que développe l'individu parce que cela lui est nécessaire. Dans cette dimension, l'oubli comporte une fonction constructive, voire réparatrice. Ainsi, on constate par exemple que le temps adoucit la douleur morale parce que l'écoulement du temps permet à l'oubli de jouer son rôle. C'est une conception soutenue par Nietzsche, pour qui l'oubli est une faculté essentielle pour le développement de l'Homme, une « faculté active […] chargée de maintenir l'ordre psychique, la tranquillité »[8]. Il est même perçu comme un phénomène vital : « Nul bonheur, nulle sérénité, nulle espérance, nulle fierté, nulle jouissance de l'instant présent ne pourrait exister sans faculté d'oubli »[9]. Pour Bergson, l'oubli conditionnerait l'état de conscience. « La conscience signifie d'abord mémoire »[10]. L'oubli viendrait donc moduler la mémoire pour « fermer de temps en temps les portes et les fenêtres de la conscience »[11]. Les psychanalystes eux-mêmes perçoivent l'oubli comme une action positive de la personne consistant en un refoulement du souvenir[12].

---

[5] Voir sur le sujet les ouvrages de P. Ricoeur, notamment, *La mémoire, l'histoire, l'oubli*, Le Seuil, 2000.

[6] C. Kossaifi, « L'oubli peut-il être bénéfique? L'exemple du mythe de Léthé : une fine intuition des Grecs », Revue pluridisciplinaire en sciences de l'homme et de la société ¿ Interrogations ? n°3, l'oubli. Décembre 2006, http://www.revue-interrogations.org/fichiers/57/mythe_de_lethe.pdf.

[7] « L'oubli », Appel à contribution, ¿Interrogations ? - Revue pluridisciplinaire en sciences de l'homme et de la société, n°3, L'oubli. Décembre 2006. Préface par le comité de rédaction. Source : http://www.revue-interrogations.org/fichiers/contrib6/Appel%20a%20contribution%203%20l%20oubli.pdf.

[8] F. Nietzsche, *Considérations intempestives*, II, 1, 1874 tr. fr. G. Bianquis, éd. Aubier-Montaigne.

[9] *Ibid*.

[10] H. Bergson, *L'Energie spirituelle*. Essais et conférences (1919), P.U.F., 2009, Chapitre I, p.34.

[11] F. Nietzsche, *Généalogie de la morale,* Flammarion, 1996

[12] Voir par exemple S. Freud, « Psychonévroses de défense », in *Névrose, Psychose et Perversion*, Paris, P.U.F.

A l'oubli, on oppose la mémoire. La mémoire est naturellement variable selon les individus mais elle est facilitée par le recours à des outils permettant à l'homme de se souvenir et de laisser des traces pour les générations futures. Fixées sur un support matériel, ces traces pouvaient disparaître par perte ou altération du support. Longtemps, les techniques disponibles pour marquer et conserver les traces ont par conséquent imposé une sélection de ce qu'il s'agissait de conserver.

L'avènement des technologies numériques et informatiques change profondément la donne et pose la question de **l'oubli numérique**. De l'analyse très fine proposée par Viktor Mayer Schönberger[13], il est possible de dégager quatre évolutions déterminantes.

Premièrement, le développement de la technologie numérique a fait apparaître une nouvelle génération de traitement, de stockage, de récupération et de partage de l'information, supérieure à ce que permettait la technologie analogique. Quels que soient l'opération et le type d'information, la digitalisation permet de reproduire fidèlement une information en utilisant un seul support et en éludant le risque d'altération. Deuxièmement, le stockage de l'information sous format numérique est aujourd'hui très largement accessible en raison d'un coût en baisse significative. Il en résulte un accroissement de la faculté de stockage et corrélativement une augmentation du coût de l'oubli dans la mesure où, en finalité, le tri des informations à conserver devient plus lourd. Troisièmement, les techniques de recherche d'informations, indispensables face au foisonnement des informations stockées, sont aujourd'hui accessibles à tous. Il en est ainsi des moteurs de recherche ou bien encore des logiciels d'indexation. Naturellement, certaines informations peuvent être d'accès limité. On songe notamment aux données du casier judiciaire. Néanmoins, elles restent accessibles à certaines catégories de personnes ce qui en garantit la mémoire. Enfin, quatrièmement, les réseaux numériques étant aujourd'hui globalisés, les informations numérisées deviennent accessibles quel que soit le lieu où l'on se trouve, par une simple connexion au réseau.

C'est un changement de paradigme. « En permettant l'avènement d'une mémoire numérique parfaite, (cette révolution numérique) a opéré un renversement de l'équilibre mémoire / oubli »[14]. Elle a « fondamentalement bouleversé le type d'information dont il est possible de se souvenir, la manière dont on s'en souvient, et à quel coût (…). De manière évidente, le souvenir est devenu la norme, et l'oubli l'exception »[15]. Faut-il condamner ce

[13] V.Mayer-Schönberger, *Delete: The virtue of forgetting in the digital age*, 2009, Princeton university press, 237 p.
[14] E. Quillet, *Le droit à l'oubli numérique sur les réseaux sociaux, mémoire*, dir. E. Decaux, 2011, p. 8.
[15] V.Mayer Schönberger, préc., p.52.

changement ? Il est *a priori* difficile de considérer que des techniques de conservation des données et d'accès à ces données constituent, en elles-mêmes, une menace pour l'homme[16]. Pour autant, cela « l'expose à une conservation intemporelle de toute trace qu'il laisserait dans la mémoire numérique et, partant, à la résurgence intempestive et dommageable d'une information qui était tombée dans l'oubli. Autrement dit, la révolution numérique n'a pas altéré le mécanisme de l'oubli, mais plutôt l'effectivité de l'oubli. Ce qui est préoccupant, ce sont donc les conséquences qui peuvent découler de ce décalage entre le passé vécu, ou ressenti, et le passé numérique : si le passé dont nous nous souvenons change et évolue sans cesse, celui inscrit dans la mémoire numérique est figé dans le temps »[17].

Lorsque la mémoire est maîtrisée par la technique, l'oubli ne peut plus jouer de la même manière, ce qui induit une approche nouvelle des comportements : il convient en effet de faire preuve d'une certaine prudence et d'avoir conscience des conséquences de la capture numérique de la mémoire. Dans ce cas, on peut être tenté par deux approches :

Ou bien l'on considère que l'équilibre mémoire / oubli tel qu'il a été établi au fil du temps en considération des capacités humaines de mémorisation doit être maintenu et l'on privilégie un contrôle extrêmement strict des activités numériques pour permettre à l'oubli de jouer le même rôle qu'il jouait lorsque la mémoire n'était pas soutenue par la technique. Ou bien l'on estime que l'évolution technologique crée une situation nouvelle, modifiant l'équilibre antérieur, à laquelle l'homme doit s'adapter, mais qu'il ne doit pas subir, parce qu'elle a été souhaitée par lui.

Présentée de cette manière, la 1ère proposition apparaît d'emblée comme régressiste. Elle va à l'encontre de l'évolution de la technique et ne correspond pas nécessairement au souhait des utilisateurs du numérique. La seconde proposition pourrait passer pour ultra-libérale ou pour une conception du laisser-faire. Néanmoins, en pareille hypothèse, les corrections ne sont pas totalement exclues mais elles seront minimales et ne se feront qu'*a posteriori*.

Dès sa création, la Commission Nationale Informatique et Liberté (ci-après CNIL) a abordé la question du droit à l'oubli dans la plupart de ses rapports annuels. Dans son 19e rapport d'activité de 1998, la Commission précisait, par exemple, que « jusqu'à l'informatisation d'une société, l'oubli était une contrainte de la mémoire humaine. Avec l'informatisation, l'oubli relève désormais du seul choix social. Le « droit à l'oubli » n'est pas nouveau ; il n'est pas né avec la loi du 6 janvier 1978, qui d'ailleurs ne le consacre pas, même s'il inspire toute notre

[16] Voir, A. Rouvroy, « Réinventer l'art d'oublier et de se faire oublier dans la société de l'information ? » *in La sécurité de l'individu numérisé, Réflexions prospectives et internationales,* S. Lacour (dir.), L'Harmattan 2010, p.249s.
[17] E. Quillet, préc. P.8.

législation. Ce droit est né avec l'idée même d'équilibre. C'est cet équilibre qu'une démocratie doit sans cesse chercher »[18].

Il existe de plus en plus d'informations numérisées concernant les individus. Ce phénomène est accentué par l'essor d'Internet. Ces informations peuvent être de natures diverses. Certaines vont permettre d'identifier l'individu et seront alors qualifiées de données à caractère personnel. D'autres demeurent très générales et ne permettent pas, *a priori*, une identification d'un individu[19].

Dans ce contexte nouveau, des individus craignent des atteintes à leurs libertés. En naviguant sur Internet, ils laissent des traces numériques[20]. Toutes ces informations ont une valeur marchande. Les services accessibles sur Internet sont de prime-abord gratuits mais doivent, d'une manière ou d'une autre, être rémunérés. Les fournisseurs de services sur Internet (sites, moteurs de recherche, réseaux sociaux, etc.) se financent grâce aux revenus publicitaires. Ainsi, pour proposer la publicité la plus adaptée, leur intérêt est de récupérer le plus d'informations possibles sur les habitudes et les envies de l'internaute. Cette information devient « la matière première du monde économique »[21]. L'on comprend alors que ces informations sont exploitées par des entreprises privées à des fins publicitaires. En passant une commande sur Amazon, les clients doivent créer un compte et communiquer des données personnelles. Par le contenu de leur commande, ils livreront des informations précieuses au fournisseur qui pourra personnaliser ses offres à leur égard. En communiquant avec leurs « amis » sur Facebook ou copainsd'avant, les membres d'un réseau social fournissent des informations qui sont passées au crible aux mêmes fins. Mais ces divulgations peuvent également se retourner contre eux lorsqu'elles concernent des données sensibles telles qu'une opinion politique ou une tendance sexuelle par exemple. C'est également le cas de données médicales qui peuvent être une source d'information pour les banques, les assurances ou bien les employeurs.

Internet constitue donc à la fois un outil de communication, d'échange et d'une certaine manière, de liberté[22], mais il permet aussi aux opérateurs économiques qui l'exploitent de se

[18] Voir le rapport d'activité 2013, p. 16.
[19] Mais voir partie III, 4., en recoupant des informations anonymes, on parvient parfois à identifier les individus.
[20] Il peut s'agir de traces volontaires ou bien involontaires. Une trace volontaire est une donnée publiée délibérément par l'internaute. Une trace involontaire est une donnée récupérée lors de la navigation sur Internet. Ce peut être une adresse IP, mais encore des mots-clés saisis dans un moteur de recherche ou bien encore des cookies, par exemple. Elles permettent, au moyen d'algorithmes spécifiques, de dresser un profil relativement précis de l'internaute.
[21] A. Belleil, *E-privacy : le marché des données personnelles : protection de la vie privée à l'âge d'Internet*, Dunod, 2001, p.11.
[22] Voir par exemple, le rapport de F. La Rue, rapporteur des Nations-Unies pour la promotion et la protection de droit à la liberté d'opinion et d'expression, A/HRC/17/27.

constituer un patrimoine informationnel à haute valeur ajoutée qui ne favorise pas l'émergence d'un droit à l'oubli.

Dans ce contexte qui met en jeu des intérêts contradictoires, il convient de tenter de définir **le droit à l'oubli.** La difficulté majeure à laquelle on se heurte lorsqu'il s'agit de définir le droit à l'oubli est la complexité de la notion d'oubli. L'oubli est en effet, avant toute autre chose nous l'avons indiqué, un phénomène psychique naturel. Par conséquent, vouloir définir un droit à l'oubli, c'est tenter de donner un sens juridique à une notion psychique. Qui plus est, lorsque le juriste envisage une application d'un droit à l'oubli aux nouvelles technologies – un droit à l'oubli numérique – il se heurte à une contradiction : il recourt à un instrument juridique pour parvenir à un résultat psychique, résultat que la technologie est précisément destinée à combattre.

D'une manière classique[23], le droit à l'oubli, tel qu'il a été envisagé dans les années 1960, renvoyait à une réalité bien précise. Il s'agissait d'un oubli imposé dans le but de garantir la paix sociale et l'ordre public. Il en est ainsi notamment des règles relatives à la prescription de l'action civile ou de l'action publique. Tout fait prescrit ne peut donner lieu à poursuite, ou à condamnation. Dans cette approche, le choix des délais de prescription semble relever davantage d'un choix de société que de la protection d'un droit de la personne. Le droit à l'oubli correspond alors au droit au respect de ces normes et apparaît comme un droit objectif[24].

Pour la Mission de recherche Droit et Justice, « actuellement, la notion de *droit à l'oubli* se définit essentiellement par sa finalité : il s'agit d'écarter tout risque qu'une personne, dont des données la concernant ont été déposées sur la toile, par elle-même ou un tiers, soit durablement incommodée par l'utilisation à son insu de ces données. Et ce, quelle que soit l'ancienneté des faits ou des données se rapportant à cette personne »[25]. On soulignera, pour rapprocher les deux droits, que c'est également par sa finalité que se définit le droit au respect de la vie privée.

Lorsqu'est invoqué le droit à l'oubli, est revendiqué **une prérogative qu'aurait l'individu d'exiger que ne soient plus accessibles à tous certains événements ou certaines données le concernant qui ne sont plus d'actualité. C'est une soustraction à la mémoire collective. Il ne s'agit cependant pas d'une soustraction totale car même si telle est la volonté de l'individu, il reste débiteur d'obligations envers la société à laquelle il appartient et peut nécessairement se heurter aux droits contraires opposés par d'autres**

[23] TGI Seine, 14 octobre 1965, note de G. Lyon-Caen, J.C.P, 1966.II.14482. Cité par R. Letteron « Le droit à l'oubli », Revue du droit public, 1996, T. CV, n°2, p. 388 note 15.
[24] Bien que certaines décisions aient admis le droit à l'oubli en tant que droit subjectif (TGI Paris, 20 avril 1983), la Cour de cassation l'a écarté, notamment, Cass. Civ. 1re, 20 novembre 1990, JCP G 1992, II, 21908, note J. Ravanas.
[25] Définition relatée dans l'appel à projet de juin 2011.

individus. Par conséquent, si un droit à l'oubli devait être consacré, il ne saurait l'être de façon absolue.

Cantonné à la problématique du numérique, le droit à l'oubli a pu être défini par la CNIL, comme « la possibilité offerte à chacun de maîtriser ses traces numériques et sa vie en ligne, qu'elle soit privée ou publique »[26]. Pour la CNIL, le droit à l'oubli résulte de l'application combinée de plusieurs principes de la loi informatique et libertés du 6 janvier 1978 et de la Convention 108 du Conseil de l'Europe du 28 janvier 1981. « Au-delà des principes de finalité, de loyauté, d'exactitude et de mise à jour des données, il s'agit de l'obligation de définir et de respecter des durées de conservation conformes à la finalité poursuivie et de prendre en compte des demandes de droit d'opposition »[27].

Cette approche juridique semble en réalité un peu trop réductrice et ne révèle pas tout l'environnement juridique d'un droit à l'oubli, ni par conséquent, l'étendue de sa problématique. Plus généralement en effet, on peut souligner qu'il existe plusieurs dispositifs juridiques qui ne sont pas désignés expressément comme étant des dispositifs de droit à l'oubli mais qui indirectement en sont inspirés ou y aboutissent parce qu'ils protègent les individus contre les débordements et les abus dans l'usage et la conservation des informations les concernant. Le droit à l'oubli n'est donc pas un concept totalement nouveau, sorti de nulle part, que l'on agiterait sous le nez de certains acteurs économiques, comme le foulard rouge devant les yeux du taureau.

D'ailleurs, concrètement, le juge, saisi d'une demande tendant à faire admettre un droit à l'oubli qui n'est pas consacré par les textes, à moins de commettre un déni de justice pour lequel il serait assurément sanctionné, ne peut pas refuser de trancher le litige sous prétexte qu'il ne dispose pas de fondements légaux adéquats. Il va donc recourir à des outils juridiques préexistants afin d'apporter la réponse qu'il estimera la plus juste possible. Or précisément, malgré le caractère inédit de certaines problématiques, le droit français et le droit international – en ce compris le droit de l'Union européenne – offrent au juge un certain nombre d'instruments, non spécialement pensés pour résoudre ces conflits nouveaux, mais qui permettront d'apporter une solution pertinente à certains différends dans lesquels le plaideur invoque un droit à l'oubli.

Il convient donc de considérer que ce n'est que dans l'hypothèse où nous estimerions que les outils juridiques actuellement disponibles, incluant ceux visés par la CNIL, n'apportent pas de solution totalement satisfaisante à ces situations inédites et problématiques, qu'il sera

[26] CNIL Rapport d'activité 2013, p. 16.
[27] *Ibid.*

possible d'envisager la création d'un droit à l'oubli autonome par rapport aux droits préexistants.

L'objet de notre étude se veut résolument large. A l'heure du tout numérique, le droit à l'oubli évoque nécessairement l'oubli numérique et renvoie au droit de l'Internet et des réseaux. Le droit à l'oubli numérique et la perception que l'on en a aujourd'hui doivent néanmoins être appréhendée largement. Tous les modes de diffusion doivent être mis en regard, tant les services de communication au public par voie électronique[28] que les supports traditionnels car les enseignements tirés des problématiques générées par les supports traditionnelles éclairent nécessairement la problématique engendrée par l'usage et le développement de nouveaux modes de communication. Il est bien évident toutefois que le développement des techniques de communication et de diffusion des informations *via* Internet et, tout particulièrement, l'essor des réseaux sociaux, donnent à la problématique du droit à l'oubli une dimension spécifique[29].

En amont, afin de mieux cibler les questions juridiques, nous avons décidé de proposer une approche sociologique du droit à l'oubli. Il s'agissait d'identifier les pratiques et les perceptions du droit à l'oubli par les intéressés. Cette perception paraissait essentielle dans la détermination de la nécessité d'un droit à l'oubli et, subséquemment, dans l'identification des outils à mettre en œuvre. Il s'agissait ici d'identifier le ressenti du public face à la conservation et à l'exploitation de données personnelles et d'informations et de mesurer la conscience qu'il peut avoir de l'impact d'une telle conservation en confrontation avec l'observation de ses pratiques.

Très rapidement, il nous a semblé évident que les analyses sociologiques et juridiques ne suffiraient pas à répondre à l'ensemble des problématiques du droit à l'oubli. Il convenait de s'assurer également de la faisabilité technique des solutions juridiques envisagées. Nous avons estimé que si un droit à l'oubli devait être consacré, il ne pourrait sans doute être véritablement garanti qu'à la stricte condition de disposer de techniques innovantes permettant une disparition effective de l'information. C'est là une problématique qui, si elle n'est pas propre à la diffusion en ligne, lui est fortement liée[30]. Cette dimension a été intégrée dans le processus d'élaboration d'un dispositif de responsabilité des fournisseurs d'Internet, et tout particulièrement, des hébergeurs[31]. Néanmoins, l'aspect informatique du problème est assez complexe parce que le

[28] Au sens large de l'article 2 de la loi nº 86-1067 du 30 septembre 1986.
[29] Voir le rapport du Groupe « Droit à l'oubli » de Cyberlex : « L'oubli numérique est-il de droit face à une mémoire numérique illimitée ? » du 25 mai 2010 et Colloque Droit de l'Internet, Cyberlex 2010, « Retour sur le rapport », Revue Lamy Droit de l'immatériel 2011, n° 71
[30] M.-P., Fenoll-Trousseau, « Les moteurs de recherche : un piège pour les données à caractère personnel », Comm. com. électr. 2006, étude 3.
[31] M. Boizard, « La responsabilité des fournisseurs d'Internet », LAMY Responsabilité, Etude 420, et « La responsabilité en matière d'Internet », Revue Droit et patrimoine 2001, n°89, p. 70 s..

point de vue le plus courant, parmi les experts du domaine, est qu'il n'est pas matériellement possible, dans le cas général, de garantir à un utilisateur que des données le concernant ont été ou seront effectivement supprimées ou rendues inaccessibles. En effet, une information digitale pouvant être copiée très facilement des milliers de fois, il semble difficile, voire impossible, de pouvoir garantir que toutes les copies d'une donnée numérique ont bien été effacées à moins de disposer d'un environnement clos très contrôlé. De plus, s'appuyer sur une responsabilité juridique des fournisseurs d'accès et des hébergeurs n'est pas forcément une solution idéale d'un point de vue informatique. En effet, leur position dans le réseau et leur rôle dans les communications ne les mettent pas toujours en mesure d'assumer techniquement la responsabilité qui pourrait leur être confiée dans ce domaine. Il est vrai cependant que des pistes théoriques existent en ce qui concerne le droit à l'oubli au prix d'hypothèses plus ou moins fortes sur l'environnement informatique dans lesquelles ces techniques sont réalisables et effectives. Il importe dès lors de les exploiter et de les enrichir pour une meilleure protection de la personne. Par exemple, des chercheurs travaillent à la conception de systèmes informatiques dans lesquels des « politiques de confidentialité collantes » sont attachées directement aux données (par exemple sous la forme de tatouage numérique), limitant ainsi l'utilisation qui peut en être faite et prévoyant une date de suppression automatique. Aussi, d'une manière plus générale, la démarche du « *Privacy by design* »[32] vise à intégrer l'aspect protection de la vie privée dès l'étape de conception des systèmes et produits par opposition à la démarche habituelle qui consiste à ajouter *a posteriori* des couches de sécurité lorsqu'un bris de vie privée est détecté.

Suivant ces différentes approches complémentaires, nous nous sommes interrogé de la manière suivante : les dispositifs juridiques et les dispositifs techniques actuels offrent-ils aux usagers les moyens de mettre en œuvre un droit à l'oubli tel qu'il vient d'être défini, ou convient-il d'aller plus loin que les prévisions actuelles et d'adopter des mesures propres à assurer un droit à l'oubli ?

Pour fournir une réponse à ces questions, il convenait de procéder en trois étapes. Tout d'abord, nous avons recherché de quelle manière était appréhendé le droit à l'oubli dans notre société (I). Ensuite, nous nous sommes attachés à cerner et à définir les contours d'un éventuel droit à l'oubli (II). Enfin, nous avons recherché comment, au-delà des principes, un droit à l'oubli pourrait-il être rendu effectif (III).

[32] Voir notamment le rapport du Groupe « Droit à l'oubli » de Cyberlex, préc.

I. L'APPREHENSION DU DROIT A L'OUBLI

Avant de nous lancer dans un questionnement juridique sur la création d'un droit à l'oubli, il était opportun de chercher à comprendre, au moyen d'une étude sociologique, de quelle manière les individus ressentent le droit à l'oubli. Quel sens a-t-il pour les utilisateurs ? Leur semble-t-il utile ? Parallèlement, nous devions nous demander si le système juridique français et européen est compatible et prêt à admettre l'existence d'un droit de cette nature. Ainsi, nous avons recherché quelle était la perception d'un droit à l'oubli par les individus (1), puis par le droit (2).

1. PAR LES INDIVIDUS

Objectifs de l'enquête sociologique – Le volet sociologique de l'étude sur le droit à l'oubli s'inscrit en amont de la réflexion juridique et technique pour comprendre les attitudes et les pratiques des usagers en matière de droit à l'oubli. On distingue en effet les attitudes et les pratiques. Les attitudes sont des connaissances, discours, pensées, représentations sociales et croyances. C'est ce que les gens pensent et savent. Les pratiques recouvrent les usages, c'est-à-dire ce que les gens font vraiment en situation.

Sur des questions de confiance et de sécurité, il existe souvent de grandes différences entre les attitudes et les pratiques qui sont intéressantes à comprendre. La différence entre les attitudes et les pratiques s'explique par le contexte, c'est-à-dire la situation : l'usager sait qu'il est dangereux de donner des informations en ligne mais il veut pouvoir bénéficier d'une vente flash, et le fait malgré tout. Il sait que Facebook ne garantit pas la sécurité des données personnelles mais comme tous ses amis partagent les photos en ligne, il le fait s'il veut les voir. On interroge alors les personnes pour comprendre les différences entre attitudes et pratiques et la manière dont ils les justifient. Par exemple, en matière de sécurité sur Internet, les usagers savent tous qu'il ne faut pas donner d'adresse personnelle mais *in situ*, motivés pour télécharger un contenu ou obtenir une information importante sur le moment, ils contournent l'interdit. Plus tard, ils le justifieront en disant que cette information était importante pour eux à ce moment-là.

Il est également essentiel de distinguer les situations personnelles et professionnelles donc différentes sphères et différents types de dispositifs techniques (Facebook, les sites des

marques…). En effet, la confidentialité des données personnelles et professionnelles peut être différente.

La démarche qualitative et inductive – La méthode retenue pour explorer des innovations et des phénomènes émergents est exploratoire qualitative par opposition aux méthodes quantitatives avec questionnaire, échantillon et intervalles de confiance. Cela pourra permettre, dans un second temps, si on le souhaite, de rédiger un questionnaire avec des items à cocher pour pondérer les observations. Mais faute d'informations précises de la réalité des usages, on ne pourrait pas définir *a priori* les items du questionnaire. Il s'agit donc d'une démarche inductive consistant à observer *in situ*, à décrire puis à modéliser les comportements. A la différence de la déduction, on ne formule pas d'hypothèses de départ.

La méthode qualitative implique un choix dans le recueil des informations. Nous retenons l'entretien qualitatif et l'observation ethnographique en situation.

1.1. L'entretien qualitatif et l'observation ethnographique

L'entretien individuel en face-à-face et l'observation permettent de capter au plus près du réel et dans l'environnement de l'usager, les comportements actuels et les évolutions de pratiques soit parce que le dispositif a changé (les règles de *privacy* ont évolué, la *timeline* a changé de forme), soit parce que la situation de l'enquêté a changé (passage à la vie professionnelle, changement de compagnon…) ou encore parce qu'un proche a fait une expérience qui impacte les usages. Les entretiens qualitatifs individuels sont dits compréhensifs car on cherche à comprendre pourquoi la personne agit de telle façon ou pense de telle manière. Il n'y a pas de bonne ou de mauvaise réponse et rien de préétabli. Les *verbatim* de l'enquêté étant importants, on enregistre les entretiens pour les retranscrire intégralement ou au moins partiellement. Nous avons fait le choix de tout retranscrire.

Le nombre de personnes à interroger n'est pas fixé comme dans la méthode quantitative par la taille de la population utilisatrice et le degré de confiance et de précision mais par l'hypothèse de saturation sémantique. On interroge des personnes jusqu'à ce qu'on n'apprenne plus rien de nouveau : on sature au niveau du sens. En général, au bout de 20-25 personnes déjà, on apprend moins de choses nouvelles. Il faut faire varier des paramètres comme ici, l'âge.

Les étapes de la méthode : il faut rédiger un guide d'entretien, le tester sur une ou deux personnes afin de le modifier au besoin puis recruter les personnes *via* les réseaux de connaissance et faire les entretiens. Ils durent environ une heure avec observation en situation. Il faut ensuite retranscrire les entretiens et les analyser en fonction des thèmes du guide d'entretien.

1.2. Le guide d'entretien

Le guide d'entretien utilisé figure en annexe 1. Il aborde d'abord les attitudes et ce que la personne sait du droit à l'oubli, puis les pratiques. Les pratiques sont abordées selon les sphères concernées (privé, professionnel, commerciale…) et les types de plateforme… Les thèmes suivants sont donc déclinés :

- Connaissance des notions de droit à l'oubli et état des lieux des connaissances sur le sujet et perception des risques
- Les fichiers de données commerciaux ou administratifs
- La sphère amicale et les médias sociaux avec Facebook, Twitter…
- La sphère commerciale
- La sphère professionnelle avec LinkedIn et Viadeo
- La sphère de partage de contenus avec Youtube et Dailymotion

Ainsi structuré, le guide d'entretien induit les thèmes de l'analyse. Nous avons choisi d'associer à l'entretien de l'observation *in situ* en observant les usagers devant leur écran en se servant des différents dispositifs. Ceci permet également d'apporter des compléments de réponse éventuels que les enquêtés pourraient oublier lors de l'entretien.

1.3. Le corpus recueilli

Les études sur le numérique (pratiques, confiance…) indiquent que les différences sont intergénérationnelles voire par fines tranches d'âge espacées de cinq ans. Il existe moins de différences de genre (homme/femme) que de génération. Afin d'observer la totalité de la diversité des pratiques et des attitudes, nous avons interrogé toutes les tranches d'âge en équipartition homme / femme, avec des actifs et des inactifs d'Ile-de-France.

Nous avons effectivement interrogé 33 personnes soit 15 hommes et 18 femmes sur un temps réduit, de mai à septembre 2012, permettant aux dispositifs d'être stables et de ne pas évoluer.

Les entretiens sont donc comparables. Le tableau suivant reprend les 33 fiches signalétiques et l'annexe 2 reprend la totalité des *verbatim* retranscrits.

Numéro	**Sexe**	**Age**	**Occupation/activité**
1	Homme	20	Etudiant en télécom
2	Femme	21	Etudiante en comptabilité
3	Homme	22	Etudiant
4	Femme	22	Etudiant
5	Femme	22	Etudiant
6	Homme	23	Ingénieur Maitrise des risques environnementaux
7	Homme	23	Etudiant
8	Homme	23	Etudiant
9	Femme	23	Etudiante
10	Homme	24	Consultant
11	Femme	24	Etudiante
12	Femme	25	RH à la SNCF
13	Femme	25	Directrice de magasin
14	Homme	25	Chirurgien dentiste
15	Homme	25	Etudiant
16	Homme	26	Employé
17	Femme	26	Etudiante
18	Femme	27	Gérante de brasserie restaurant
19	Femme	27	Assistante de direction
20	Femme	28	Assistante de direction
21	Femme	29	Etudiante en psychologie
22	Homme	34	Architecte
23	Femme	35	Chef de produit senior
24	Homme	35	Graphiste
25	Homme	36	Cadre commercial
26	Femme	37	Chef de produit senior

27	Femme	47	Commerciale
28	Femme	51	Libraire
29	Femme	55	Enseignante et consultante
30	Homme	55	Directeur d'unités opérationnelles
31	Femme	55	Femme au foyer
32	Homme	58	Consultant en RH
33	Homme	61	Cadre dirigeant

1.4. Les résultats de l'analyse des entretiens

1.4.1. Les attitudes face au droit à l'oubli

Connaissance du concept de droit à l'oubli :

L'expression « droit à l'oubli » n'est pas connue des usagers. Si on leur demande ce qu'elle peut vouloir dire, ils pensent au droit « de se refaire une virginité », au droit « à l'omission » ou de « raconter son histoire comme on a envie », de ne pas tout raconter de soi, d'oublier certaines relations amoureuses pour se refaire un CV amoureux moins rempli. Le terme évoque plutôt des épisodes de la vie que l'on ne souhaite pas médiatiser parce que l'on a évolué et vieilli. Il s'agit du droit d'évoluer, de s'adapter, de changer de look.

Ce droit à l'oubli semble **toujours une nécessité et un droit indispensable**. On doit pouvoir « repartir à zéro » et « avoir le droit de ne pas tirer avec soi des boulets à vie ». Il se confond avec le droit à l'erreur. On doit pouvoir bénéficier de la tolérance des gens qui oublient des épisodes de votre vie. Certains expliquent que suite à une rupture (« j'ai été quittée »), ils ont eu besoin de voir d'autres personnes pour ne pas toujours être assimilée « à la fille qui a été plaquée ». Lorsqu'ils abordent les pratiques numériques, c'est aussi ce cas qui arrive massivement : « j'ai demandé à mon ex de supprimer des photos de nous sur sa page Facebook ». Ils ne citent pas le numérique. Il n'arrive que lorsqu'on les interroge encore et qu'ils se disent qu'il doit « falloir en parler ou faire le lien avec Internet ».

On observe peu de différences de genre (H/F) ou d'âge.

Concept de trace numérique et de protection de la vie privée

L'expression « traces numériques et protection de la vie privée» est mieux connue ou se comprend d'elle-même. Elle est de fait directement liée au numérique. Mais les risques perçus sont surtout ceux liés aux « cookies » et « aux enregistrements que gardent les ordinateurs » et « à l'usurpation d'identité » dont tout le monde a entendu parler. Certains évoquent les traces liées aux cartes bleues, à la géolocalisation, au fait qu'on puisse maintenant nous retrouver où qu'on aille et retracer nos achats et notre parcours. L'usurpation d'identité revient régulièrement parce que les gens ont vu des reportages à la télé ou dans les journaux sur ce sujet. La numérisation des fichiers et le recours à des serveurs vocaux ou à des transactions numériques provoquent ce genre de problèmes. Mais les autres problèmes liés au numérique sont peu perçus.

La protection de la vie privée concerne essentiellement les photos. On observe une différence selon l'âge. Les plus jeunes sont mieux informés des risques liés aux photos et informations sur Facebook. Ils sont sensibilisés aux risques dans leur recherche de stage ou d'emploi car ils savent que les employeurs vont chercher leurs informations sur Internet. Ils savent qu'il faut éviter de mettre des photos d'eux dans des soirées alcoolisées ou peu vêtues. Mais cela ne veut pas dire qu'ils ne le font pas.

Les plus âgés perçoivent surtout les risques venant de l'extérieur : l'ordinateur qui garde des traces et des cookies mais voient peu le risque lié à ce qu'eux pourraient laisser comme informations. Leur logique est « je mets peu ou pas de photos donc je ne cours pas de risques ». Tous ont le sentiment d'être impuissants face aux acteurs que sont Google ou Facebook qui changent régulièrement leurs conditions de confidentialité.

Les mauvaises expériences

Les jeunes ont tous fait de mauvaises expériences liées aux photos sur Facebook surtout dans le cadre de soirées arrosées ou lors de rupture amoureuse où leur ancien compagnon laissait des photos du couple. Hors de la sphère privée, ils ont parfois été témoins de mauvaises expériences dans le cadre professionnel : un nouvel embauché avait déjà une mauvaise réputation et n'est pas resté ou tel autre n'a pas été embauché.

La sensibilisation

Elle est faible, essentiellement dans les médias qui vont exposer les cas extrêmes sans préciser leur fréquence. Il s'agit de cas parfois rares et atypiques mais ce sont les plus médiatisés. Les plus jeunes ont eu une éducation de la part des parents qui les sensibilisent aux risques mais de façon anxiogène sans être eux-mêmes experts du numérique et donc sans pouvoir apporter de solutions autre que la solution extrême qui consiste à dire « clôturer votre compte Facebook ». Ils disent que leurs jeunes frères et sœurs ont eu une sensibilisation en classe mais pas eux.

1.4.2 Les fichiers de données personnelles

Définition et tiers détenteurs

La définition d'un fichier de données personnelles est bien connue : il s'agit d'une base de données d'informations personnelles sur les clients ou des usagers détenue par un organisme tiers. Les fichiers de données sont associés aux entités commerciales ou étatiques (impôts, sécurité sociale…). Les personnes interrogées disent qu'il faut se méfier des entreprises qui peuvent revendre les données et moins de l'Etat. Ils ont constaté avoir des appels entrants de centres d'appels, des entités qu'ils ne connaissent pas mais qui ont eu leurs coordonnées par une autre entreprise qui a vendu le fichier.

Durée de conservation

La durée de conservation est mal connue. Soit ils la pensent infinie, soit de un an, soit jusqu'à la clôture du compte mais rien de précis n'est connu. La bonne durée de conservation des données serait jusqu'à la clôture du compte avec suppression ensuite ou encore un an renouvelable par mail de l'usager. Les informations sur la durée de conservation des informations et l'accès aux données personnelles sont opaques et les entités tierces ne communiquent pas dessus. Les seules tentatives et expériences en la matière concernent les newsletters pour se désabonner. Ceci fonctionne bien. Certains connaissent l'obligation légale *d'opt-in*. Pour le reste, peu de chartes précises ont été vues sur les sites ou en magasin.

Confidentialité des données

Les usagers font des différences entre les données qu'ils acceptent de donner et celles qu'ils refusent de transmettre. Nom et prénom, jour de naissance sans année, adresse postale

sont données sans réticence. Ils disent donner au cas par cas : date de naissance, situation maritale, adresse mail, numéro de portable, numéro de fixe, nombre et âge des enfants, profession, centres d'intérêts. Et affirment ne jamais donner : coordonnées bancaires, revenu mensuel, orientation religieuse, politique, sexuelle, prison, drogue, téléchargement illégal.

Au-delà de la catégorie de données, tout dépend de la légitimité à connaître l'information : pour payer un billet en ligne, il est normal de donner son numéro de carte bleue. Pour un site de sorties et de mise en relation entre personnes, il est normal d'indiquer des centres d'intérêts. Pour bénéficier de promotions ou de bons de réduction sur des sites, il faut fournir des informations sur son lieu d'habitation, l'âge des enfants, la race du chien qu'on possède. Si on veut retrouver des amis d'enfance, il faut indiquer le lycée qu'on fréquentait… C'est la légitimité qui détermine si on transmet ou non l'information. Sur les réseaux sociaux c'est différent : la donnée apparait publiquement sans bénéfice immédiat ou différé.

1.4.3. Facebook

L'usage de Facebook est très répandu et quotidien ou pluri quotidien pour les moins de 40 ans. Il sert à communiquer avec les amis, la famille, échanger des photos, partager et réagir. Il ne semble pas exister de différence de genre mais une différence de génération au niveau des pratiques Facebook notamment sur le type de contenu partagé et commenté.

Pour les jeunes, Facebook constitue une extension de la cour de récréation où ils commentent les soirées, les activités faites dans la vie réelle. Ils parlent entre proches de leur quotidien partagé comme MSN auparavant. Les plus âgés (les parents et les plus de 40 ans) mettent et commentent les informations des autres médias plus anciens. Ils mettent un lien vers un podcast d'émission qu'ils ont aimé à la radio, commentent une émission de télé ou un fait d'actualité (affaire Dominique Strauss Kahn, tweet de Valérie Trierweiller…). Pour les jeunes, la communication sur Facebook est centrée sur le réseau social et ses activités. Pour les plus âgés, cette communication est liée à la sphère publique et médiatique classique (radio, TV, actualité) avec pour thèmes la politique, l'économie, l'actualité nationale ou internationale (people inclus) et très peu à leur activité privée. Par conséquent, les risques pour la vie privée ne sont pas les mêmes pour les deux tranches d'âge.

Les amis Facebook sont quasi toujours connus de la vie réelle, au pire vus une seule fois. Ils ont demandé à devenir amis sur Facebook et l'interviewé n'a pas osé refuser. Cela peut

servir, on ne sait jamais. Tous sont satisfaits de garder une trace pour une utilisation potentielle ultérieure. C'est une fonction mémorielle sans forcément échanger quoi que ce soit en ligne.

Une pratique de droit à l'oubli dépend du genre. Le *tag* de photos est fréquent chez les jeunes et le *détag* aussi parce qu'on n'est pas à son avantage. Ce point est essentiellement féminin.

Les interviewés se disent attentifs à ce qu'ils inscrivent sur le mur des autres en se demandant s'ils aimeraient qu'on écrive cela sur le leur. Les amis écrivent sur les murs (ou *timeline*) et il faut parfois réduire les autorisations notamment entre parents et enfants. Les parents mettent des messages de soutien ou des photos des enfants bébés que les enfants devenus adultes ne veulent pas voir. Il s'agit de la transposition de ce qui se passe avec des adolescents qui aiment être conduits au lycée en voiture mais demandent à être déposés 100 mètres avant. Certains ont modifié les autorisations d'accès toujours dans le sens de la restriction suite à de mauvaises expériences : soit au cas par cas en excluant des personnes qui ont publié des infos trop personnelles en mélangeant les sphères ; soit parce qu'ils approchent de l'entrée dans la vie professionnelle. Ce moment semble particulier car c'est là que se posent les premières questions s'ils s'en posent. Certains ont pu bloquer leur maman parce que celle-ci écrivait « mon bébé », « ma petite chérie » sur le mur. Le paramétrage des options est souvent limité aux amis mais la politique de Facebook parait floue et changeante donc les interviewés font preuve de fatalité. Il faudrait une expertise qu'ils n'ont pas toujours. De toutes façons, Facebook est gratuit et doit gagner de l'argent donc c'est une contrepartie.

1.4.4. Sites de marques

Unanimement, les personnes interrogées ont confiance dans les sites dont ils connaissent les marques soit parce qu'il y a des magasins physiques soit parce que la marque est déjà bien connue et jugée fiable. Pour les sites, *pure player*, encore peu connus, la méfiance règne. L'indice « cadenas » ou « https » peut suffire à rassurer mais pas toujours. La réputation dépend de la notoriété et du bouche à oreilles. Les avis des internautes inconnus pèsent peu lorsqu'on ne connait pas le site. Ils importent lorsqu'on fait confiance à un site, pour le choix d'un article plutôt qu'un autre. Par exemple un hôtel ou un mobile ou pour suggérer un article que des internautes qui ont acheté le même produit A que vous ont aimé et aussi acheté ou encore ont hésité avec celui-là.

Savoir ce que les entreprises savent sur eux n'est pas une préoccupation même si les internautes remarquent que les sites mémorisent leurs achats et leurs préférences ou que Google leur propose des liens sponsorisés en rapport avec ce qu'ils ont regardé les fois précédentes. Les internautes sont enregistrés sur différents sites et ont des cartes de fidélité numériques mais ne les utilisent pas forcément. Ces comptes et cartes ont été créés une fois au départ ou lors d'un achat et les internautes oublient les informations pour les réutiliser ensuite.

Il serait pertinent que les entreprises conservent les informations et permettent d'y accéder spontanément sans avoir à mémoriser des tas d'informations. Par exemple sur voyagessncf.com, les miles ne sont souvent pas accumulés car les internautes oublient les mots de passe. Cette charge cognitive devrait être portée par les entités commerciales.

1.4.5. Sphère professionnelle

Il existe des réseaux professionnels tels LinkedIn ou Viadeo. Les plus jeunes ont tous un compte professionnel, soit Viadeo (plus français) soit LinkedIn (plus international) soit les deux sauf dans le cas où ce n'est pas pertinent selon eux comme le chirurgien-dentiste (pour jeune) ou le libraire. Les craintes par rapport aux informations personnelles sont rares. Toutes les informations demandées semblent légitimes et motivées par la recherche d'emploi ou l'entretien du réseau. Là encore, les informations demandées par les sites professionnels semblent légitimes et ne donnent lieu ni à refus, ni à hésitations.

1.4.6. Pratiques ludiques et sites de partage

Les pratiques de partage de contenus sur You tube ou Dailymotion sont limitées à la consultation et au réacheminement à des amis pour partager des contenus. Les cas où les internautes déposent des contenus sont motivés par une diffusion de musique pour se faire connaitre ce qui correspond exactement aux bénéfices retirés de ces sites à savoir la gratuité et la visibilité.

En conclusion, l'étude sociologique révèle que les individus sont conscients des conséquences de l'usage d'Internet sur la protection des données et informations les concernant mais ils font état d'une sorte de fatalisme. Cette situation peut sans doute s'expliquer par la difficulté que certains éprouvent à comprendre de manière très précise les mécanismes limitant l'usage de leurs données. Elle s'explique également par le souhait exprimé par les usagers de

pouvoir continuer à bénéficier des services gratuits proposés en ligne parce qu'ils leur apportent des avantages. Le bénéfice de ces services justifie qu'ils acceptent certains risques liés notamment au recueil de leurs données.

Les questions demeurent toutefois nombreuses pour le juriste et notamment celle de savoir jusqu'où les usagers sont-ils prêts à aller pour pouvoir utiliser les services qui leur sont proposés. Il n'est pas certain que tous les enjeux aient été bien intégrés dans la démarche d'enquête notamment en ce qui concerne la diffusion de certaines données sensibles comme des données médicales ou judiciaires par exemple – il est question dans les résultats de l'enquête de données exploitées par l'Etat mais, sans précision, les usagers ont peut-être eu des difficultés à identifier le type de problématique que cela pourrait leur poser. D'ailleurs, les personnes interrogées ont immédiatement songé aux données et traces qu'elles laissent elles-mêmes sur Internet et, peu de cas est fait des données qui sont collectées par des tiers sans leur accord préalable, ce qui est le cas des données judiciaires que l'on retrouve sur des bases de données – parfois en libre accès – ou dans les fichiers informatisés de l'administration judiciaire. Pourtant, l'accès à ces données peut être extrêmement préjudiciable à la personne qu'elles concernent et méritent d'être intégrées dans une réflexion sur le droit à l'oubli.

Par conséquent, l'enquête témoigne surtout de la conscience des jeunes en particulier d'être prudents dans la diffusion de certaines données. Il reste toutefois difficile de mesurer jusqu'où s'étend cette prudence.

L'afflux des demandes de déréférencement adressées à Google à l'annonce, le 30 mai 2014, de la mise à disposition des internautes européens d'un formulaire destiné à permettre une désindexation (40000 demandes au 2 juin 2014, 146000 au 15 octobre de la même année, 20 % étant des demandes françaises) démontrent toutefois que certaines informations présentes sur Internet les dérangent ce qui ne ressort pas si nettement que cela de l'enquête menée. Cela peut sans doute s'expliquer par le fait que la procédure est ouverte par l'un des plus gros moteurs de recherche au monde, ce qui constituera une des pistes à explorer tant dans l'approche juridique que technique d'un droit à l'oubli.

2. PAR LE DROIT

Le concept de droit à l'oubli est, à notre sens, plus large que ce qu'imaginent les usagers sondés pour les besoins de l'enquête sociologique. Il est d'ailleurs consacré de manière éparse dans différents domaines du droit, de façon directe ou indirecte.

De façon indirecte, le droit à l'oubli est sous-jacent dans les mécanismes de prescription extinctive et dans certains principes protecteurs de la personnalité. Ainsi la prescription éteint le droit de celui qui pouvait exercer un droit en justice et qui ne l'a pas fait dans le temps prévu par la loi. La règle est justifiée en droit civil par des motifs de paix sociale, d'ordre public et de sécurité juridique. En droit pénal, en revanche, elle est dictée par le droit à l'oubli[33]. De même, les droits fondamentaux de la personne tels que le droit au respect de la vie privée garanti par les articles 9 du Code civil, 7 de la Charte européenne des droits fondamentaux et 8 de la CEDH, permettent à la jurisprudence de condamner des pratiques allant à l'encontre du droit à l'oubli[34]. Ce droit est renforcé par le dispositif découlant de la loi n° 2004-575 du 21 juin 2004, pour la confiance dans l'économie numérique et le droit de la communication, dite LCEN, qui offre aux personnes victimes de contenus illicites diffusés sur Internet, notamment ceux qui violent leur vie privée, le droit d'agir contre l'hébergeur du site pour obtenir la suppression du contenu.

De façon directe, la loi dite informatique et libertés du 6 juillet 1978 renvoie à l'idée d'un droit à l'oubli se traduisant par une durée de conservation des données personnelles n'excédant pas « la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées » et un droit de retrait ou un droit d'opposition à l'utilisation de ces données. C'est là encore, l'un des fondements privilégiés par la jurisprudence pour reconnaître un droit à l'oubli.

Bien que sous-entendu dans l'ordre juridique, le droit à l'oubli est néanmoins conçu pour faire face à des situations particulières. Il convient donc de se demander si une telle approche permet de répondre à des situations inédites.

Dans son appel à projet, la mission de recherche Droit et justice évoquait le fait que le « *droit à l'oubli* pose également la question de l'affirmation d'un éventuel *droit de propriété* des individus sur leurs données personnelles - au-delà des aspects tenant à leur durée de vie et à leur confidentialité - dont les implications devraient être précisément évaluées ». Comme nous venons de le souligner, le droit comporte depuis longtemps des mécanismes juridiques de droit à l'oubli. Le droit de propriété a un temps été envisagé par l'équipe mais d'emblée il est apparu que le caractère absolu et exclusif de ce droit ainsi que ses attributs, entraient en contradiction

[33] C. Costaz, « Le droit à l'oubli », Gaz. Pal 1995, p. 961. R. Merle et A. Vitu, *Traité de droit criminel*, Procédure pénale, 4è ed., Cujas, n° 818.
[34] Notamment, CA Paris 15 sept. 2000 : Gaz. Pal. 2001, n° 270 p.18. Cass. Civ. 1ère, 7 mai 2008, D. 2008, AJ 1481, J. Hauser

totale avec les prérogatives nécessairement reconnues aux tiers sur les données personnelles. Le droit de propriété devrait subir tellement de restrictions, qu'il en serait profondément dénaturé. Une telle approche ferait également voler en éclat les grands principes du régime actuel de protection des données à caractère personnel, régime conçu spécialement pour ces données et dont les règles permettent de concilier les droits de la personne et les droits des tiers. Il faut ajouter que pour l'essentiel, les données personnelles sont des faits et l'on n'imagine pas qu'un droit de propriété puisse couvrir des faits[35].

A vrai dire, si le droit à l'oubli prend une dimension totalement inédite avec l'avènement du numérique et d'Internet, il trouve ses racines profondes dans des mécanismes juridiques éprouvés qui permettent d'entamer une réflexion sur les possibilités d'un droit à l'oubli. Historiquement et fondamentalement, c'est sans doute le droit de la prescription qui illustre le mieux la façon dont le droit, en tant que phénomène social et outil d'organisation sociétale, intègre le droit à l'oubli (2.1). En jurisprudence, c'est en revanche le droit au respect de la vie privée qui a été privilégié en tant que cadre du droit à l'oubli (2.2). Mais de façon plus contemporaine et plus spécifique, le droit à l'oubli sous-tend et est intimement lié au dispositif de protection des données personnelles (2.3).

2.1. Droit à l'oubli et droit de la prescription

Le droit de la prescription repose sur un élément essentiel, le temps. C'est là, nous semble-t-il, une caractéristique qu'il partage avec le droit à l'oubli. Aussi, en identifiant les fondements et les mécanismes de prescription, il devient possible d'imaginer quel rôle y a joué le droit à l'oubli et, subséquemment, quel rôle il pourrait être amené à jouer dans nos sociétés modernes.

« La réflexion philosophique qu'il y a trop de droit, à tout le moins trop de droit en action, trop de contentieux, justifierait une politique générale de réduction des délais. A l'inverse, la conviction que le mal est partout, ainsi que le mensonge qui le dissimule, conduirait à l'allongement, sinon à l'imprescriptibilité. Entre les deux tendances, les législateurs oscillent au gré de leurs préférences du moment (…) Le droit est capable d'un maniement arbitraire du temps »[36]. En ces quelques mots, Carbonnier exprime toute l'ambiguïté de la relation du Droit avec le temps et, par voie de conséquence, avec l'oubli. L'utilisation de la prescription, comme moyen d'effacement de certains faits ou actes de la mémoire juridique, pâtit de cette imprévisibilité, de cette impression de désordre. En droit pénal, la prescription de l'action

[35] Comparer avec la protection du savoir-faire qui ne peut être assurée par un droit de propriété, fût-elle intellectuelle.
[36] J. Carbonnier, *Droit des obligations*, PUF, pp. 627-628

publique repose sur l'idée que « passé un certain délai, il est superflu de rappeler en justice les crimes qui ont été oubliés et dont les effets ont disparu »[37]. L'idée partagée au XVIIIe siècle est le « délai qui s'écoule avant que la prescription ne soit acquise est la « peine naturelle du crime », temps passé dans le remord et la crainte d'être découvert et puni ce qui justifierait que le principe s'applique aussi aux crimes secrets »[38]. On parle de la « grande loi de l'oubli ».

La présentation d'une vision d'ensemble cohérente de notre Droit de la prescription est un exercice délicat. Ce droit est pris entre des vents contradictoires, celui de l'oubli ou au contraire celui de la mémoire, au gré des époques ou des tendances politiques au pouvoir. Le droit à la prescription n'est donc pas à l'abri de préoccupations catégorielles et circonstancielles.

Les lois d'amnistie et les grâces présidentielles expriment bien cette idée que l'oubli est en partie lié à la volonté du pouvoir. Leur opportunité relève en effet de la seule appréciation du Président de la République. Manifestement, ces dernières années, elles ne sont pas dans l'air du temps. Il n'est en effet pas anodin que nos deux derniers Présidents de la République messieurs Sarkozy et Hollande, n'en aient pas fait usage lors de leur prise de fonction, comme il est de coutume de le faire. La politique actuelle n'est ni au pardon, ni à l'oubli que les citoyens ne toléreraient prétendument pas.

Le droit à l'oubli par le vecteur de la prescription est donc à degré variable. Certains faits n'ont pas vocation à être oubliés. Tout ne peut s'effacer des mémoires. A l'inverse, d'autres faits doivent pouvoir disparaître rapidement afin de favoriser la paix sociale et la sécurité juridique. Entre ces deux extrêmes, le droit opte pour une durée de prescription de droit commun, susceptible d'embrasser une majorité de cas.

2.1.1. Le droit commun de la prescription

Il existe des règles de principe, tant en droit civil qu'en droit pénal, qui ont vocation à appréhender la majorité des hypothèses. Un droit commun en quelque sorte de la prescription. Si en droit civil, la tendance contemporaine semble à la réduction du délai de prescription et donc à la promotion d'un droit à l'oubli, il en va différemment en droit pénal.

En droit civil, la tendance est à la réduction des délais. La loi du 17 juin 2008 a ainsi œuvré clairement en faveur de la diminution des délais de droit commun, jugés trop longs. Le projet qui animait la loi du 17 juin 2008 était ambitieux. Il s'agissait non seulement de remédier

[37] J. Danet, *La justice pénale entre rituel et management*, PUR 2010, p. 123 se référant à S. Pufendorf, *Le droit de la nature et des gens* (édition de Bâle 1732), IV, 12, 1-2, Caen, Centre de philosophie politique et juridique, 1987, t. 2, pp. 589-592.
[38] *Ibid*.

au foisonnement de notre droit, mais aussi d'en assurer une lisibilité, notamment au niveau international.

Le délai de droit commun est passé de 10 ou 30 ans à 5 ans. Cette durée tend à instaurer un équilibre jugé satisfaisant entre le risque d'insécurité juridique et celui d'injustice pour les titulaires de droits qui ne disposeraient pas d'un laps de temps suffisant pour les faire valoir.

Cette réforme présente également le mérite d'harmoniser les délais. Ce nouveau délai s'applique en effet, sauf disposition dérogatoire, aux actions contractuelles comme délictuelles, aux personnes civiles comme aux commerçants. Cette simplification est heureuse[39] mais le législateur peine à aller jusqu'au terme de sa logique en droit civil.

Certains domaines, jugés plus dignes de protection que d'autres, jouissent d'un délai de prescription plus long. Ainsi en est-il de la prescription des actions des victimes directes ou indirectes de dommage corporel (C. civ., art. 2226)[40].

A mesure que l'intérêt protégé est essentiel, la durée de prescription s'allonge. C'est le cas lorsque le préjudice est causé par des actes de barbarie, ou par des violences ou des agressions sexuelles commises contre un mineur (C. civ., art. 2226 al. 2).

Enfin, on observera que le raccourcissement des délais, voulu par le législateur de 2008, s'accompagne d'un report du point de départ et de l'extension du domaine des causes de suspension ou d'interruption de la prescription. Par le jeu de ces règles, la durée de prescription excédera bien souvent les 5 ans initialement escomptés. Par exemple, le point de départ de ces actions est « flottant », « glissant ». Il dépend d'un élément subjectif qu'est la connaissance des faits par la personne souhaitant agir. Le juge aura une grande liberté pour sa mise en œuvre, tant en ce qui concerne l'appréciation des faits nécessaires à l'exercice du droit qu'en ce qui concerne celle de leur connaissance par leur titulaire.

En droit pénal, la tendance n'est pas aussi nette. Le droit commun repose sur le triptyque : 3, 5 ou 10 ans selon que l'infraction est une contravention, un délit ou un crime. Toutefois le législateur ne cesse de multiplier les dispositions exceptionnelles, à tel point que

[39] En outre, à l'image du régime de responsabilité du fait des produits défectueux fondé sur les articles 1386-1 et suivants du Code civil, la loi instaure un délai butoir de 20 ans. C'est-à-dire qu'au terme de cette durée, plus aucune action n'est envisageable. L'article 2232 alinéa 1 du Code civil énonce que « le report du point de départ, la suspension ou l'interruption de la prescription extinctive ne peut avoir pour effet de reporter le délai de la prescription extinctive au-delà de 20 ans à compter du jour de la naissance du droit ». D'un point de vue juridique, les faits disparaissent définitivement. Le droit à l'oubli fait son office.

[40] Elles peuvent introduire une action dans les dix ans à compter de la consolidation de leur dommage. Ce délai est particulièrement long, tant la consolidation de certaines maladies peut être tardive. Il frise même la perpétuité pour certaines pathologies qui ne sont pas susceptibles de consolidation. Cette règle traduit sans conteste la préoccupation qui anime notre droit contemporain de réparer le dommage corporel.

« le régime de droit commun de la prescription des infractions pénales est devenu difficilement compréhensible »[41].

Surtout, la légitimité de l'oubli comme fondement de la prescription pénale n'apparaît plus dans notre société comme une loi sociale si évidente[42]. La Cour de cassation, elle-même, affirme depuis plusieurs années son hostilité à la prescription de l'action publique : la doctrine en fait unanimement le constat de longue date. L'extinction de l'action publique que la prescription engendre par suite de l'impunité de fait dont a joui pendant un certain temps l'agent est regardée avec défaveur par la jurisprudence, rejointe au demeurant par une partie de la doctrine, ce alors même que les effets de l'institution ont été atténués par l'abrogation, en droit commun, du principe de solidarité des prescriptions des actions publique et civile. La Chambre criminelle a donc défini puis mis en œuvre une véritable politique criminelle de mise en échec de l'institution, sinon dans son principe même, du moins dans ses modalités d'application. La détermination du point de départ du délai de prescription[43] est l'un des points d'équilibre de l'institution sur lequel s'est exercée de manière privilégiée cette politique prétorienne.

Au-delà de ce socle de la prescription, le législateur consacre un certain nombre d'exceptions.

2.1.2. Les exceptions

Certains faits, par nature exceptionnels, ne peuvent et ne doivent être effacés. Le droit à l'oubli est alors impossible. Bien souvent, il s'agit d'événements qui n'appellent pas le pardon, même s'il n'y a pas de corrélation directe entre ces deux phénomènes. Quelle que soit leur antériorité, leurs auteurs doivent en répondre. D'autre part, certains droits sont intimement liés

[41] M. Veron, Revue Dr. Pénal 2006, comm. 110.
[42] J. Danet, *La justice pénale entre rituel et management*, PUR 2010, p. 131.
[43] Qui ne se peut prescrire ni avant d'être consommée ni avant d'avoir fini de se consommer.

à la personne, de sorte qu'ils ne sauraient s'effacer. On songe aux crimes contre l'humanité dans la première hypothèse[44], au droit de propriété dans la seconde[45].

A l'opposé, certains faits ne sont susceptibles d'être appréhendés par le droit que dans un laps de temps réduit. A leur égard, le droit à l'oubli est renforcé. Il s'agit essentiellement d'une question de politique juridique, éventuellement motivée par des raisons matérielles. Ainsi des infractions de presse. Soucieux de préserver la **liberté de la presse**, le législateur a échafaudé un régime de responsabilité sévère mais enfermé dans des délais de prescription très courts. Ce délai est en principe de trois mois à compter du jour de la publication litigieuse. Passée cette date, plus aucune action en justice n'est envisageable. Exceptionnellement, ce délai est porté à un an, pour des faits jugés plus dignes de protection par le législateur. Ainsi aux termes de l'article 45 de la loi du 9 mars 2004, qui a introduit un article 65-3 dans la loi de 1881, ce délai s'applique aux délits de provocation à la discrimination, à la haine ou à la violence raciale ou religieuse, de contestation des crimes contre l'humanité, de diffamation et d'injure à caractère racial ou religieux. Etant donnée la brièveté de ces délais, la jurisprudence fait une application stricte de ces textes qu'elle n'applique qu'aux seules infractions de presse au sens de la loi de 1881.

En conclusion, le droit de la prescription témoigne de la prise en compte du concept d'oubli par le droit mais n'offre pas une grille de lecture limpide de la place du droit à l'oubli dans notre société contemporaine. Si la volonté semble être à la réduction des délais de prescription, afin peut-être de s'adapter à l'accélération du temps de nos sociétés[46], cette

[44] Vestige de notre passé jugé intolérable, les crimes contre l'humanité sont imprescriptibles. Ceux-ci englobent les crimes contre une personne en raison de son appartenance à un groupe de personnes, en la traitant comme si ce groupe n'appartenait pas à l'humanité. Il repose donc sur la négation d'un groupe et des personnes supposées appartenir à ce groupe. Répondent à cette qualification le génocide, les actes de persécution visés par l'article 212-1 du Code pénal, les crimes de guerre aggravés ou encore la participation à un groupement en vue de la participation à un crime contre l'humanité. Ainsi que le dispose l'article 213-5 du Code pénal, « l'action publique relative aux crimes prévus par le présent sous-titre, ainsi que les peines prononcées, sont imprescriptibles ». Cette imprescriptibilité est apparue naturelle à la suite des crimes commis pendant la Seconde Guerre mondiale. Elle fut inscrite dans le statut du Tribunal militaire de Nuremberg, reprise par la suite dans les conventions internationales et le droit français. Il est donc universellement admis qu'il serait intolérable que les responsables de ces crimes puissent demeurer impunis à raison du jeu du temps.

[45] Droit « sacré » selon les rédacteurs du Code civil, il est de principe que ce droit ne s'éteint pas par l'écoulement du temps. La qualité de propriétaire demeure, bien qu'il n'en soit pas fait usage. Le droit de propriété est perpétuel. Ce caractère peut prendre appui sur l'article 2 de la Déclaration des droits de l'homme et du citoyen qui affirme que le droit de propriété est un droit naturel et surtout imprescriptible de l'homme : « le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'Homme. Ces droits sont la liberté, la propriété, la sûreté, et la résistance à l'oppression ». L'imprescriptibilité est un moyen de sauvegarder la propriété privée, en interdisant l'attribution d'un bien laissé en déshérence à l'Etat. On trouve là encore un vestige de notre passé, de cette époque où régnait la crainte d'un Etat tout puissant. L'imprescriptibilité prévaut quelles que soient la nature et les modalités du droit de propriété. Ainsi les droits moraux attachés à la propriété littéraire et artistique sont perpétuels, inaliénables et imprescriptibles selon l'article L. 121-1 du Code de la propriété intellectuelle. Les droits patrimoniaux sont quant à eux prescriptibles, même si certains auteurs ont relevé que « la temporalité est sans cesse repoussée », qu'il y aurait « un fait de la perpétuité » (J.-M. Bruguière, « Faits et méfaits de la perpétuité dans la propriété littéraire et artistique », Propriété industrielle oct. 2010, dossier 10)

[46] H. Rosa, *Accélération*, La découverte, 2013.

convergence n'est pas lisible. Certains domaines s'y montrent réticents : particulièrement ceux qui touchent directement à l'humain, voire à l'humanité. A l'opposé, ceux directement en lien avec les aspects mercantiles de nos sociétés tolèreraient un oubli plus rapide. Cette analyse permet de pressentir une difficulté liée aux modalités d'un droit à l'oubli, celui de la dimension temporelle. En droit de la prescription, la donnée temporelle est en étroite liaison avec la finalité de la prescription. Par conséquent, à finalité différente, délai différent. Si c'est cette logique qui doit inspirer le législateur dans la construction d'un droit à l'oubli, on pressent un dispositif complexe. En réalité, il n'y a pas de corrélation directe entre le temps de la prescription et le temps de l'oubli parce qu'ils obéissent à des logiques différentes. Certes, les deux mécanismes répondent à une exigence de paix sociale mais le droit de la prescription extinctive libère un débiteur, face à un tiers ou face à la société, parce que l'intérêt à protéger a perdu de sa vigueur. Ce n'est pas le cas du droit à l'oubli tel que nous l'avons défini. A certains égards, on peut considérer que le droit à l'oubli opère comme une prescription acquisitive. C'est un droit qui nait au bout d'un certain temps. Néanmoins, la comparaison s'arrête là car le droit à l'oubli ne conduit pas à un transfert de droit d'un opérateur vers la personne concernée par une information. Le droit de l'opérateur cesse simplement, sans opérer de transfert. Le droit de la prescription est donc en partie inspiré du droit à l'oubli mais un droit à l'oubli ne saurait se construire sur le modèle du droit de la prescription.

2.2. Droit à l'oubli et droit au respect de la vie privée

Le droit à l'oubli est traditionnellement perçu comme l'un des pendants du droit au respect de la vie privée consacré par l'article 9 du Code civil, l'article 7 de la Charte européenne des droits fondamentaux et l'article 8 de la CEDH. Pourtant, il n'est pas certain que ce fondement soit idéal.

Une première différence distingue le droit au respect de la vie privée et le droit à l'oubli, le critère temporel. Le temps paraît être une composante nécessaire et caractéristique du droit à l'oubli. Il n'est pas, en revanche, un critère de qualification du droit au respect de la vie privée. C'est un trait qui marque l'une des limites du droit au respect de la vie privée comme fondement du droit de la personne à s'opposer à l'exploitation de faits la concernant. C'est ce facteur temps qui explique qu'un fait public puisse être protégé par le droit à l'oubli alors qu'il ne saurait l'être par le droit au respect de la vie privée. Mais inversement, cela signifie aussi qu'un même fait peut tantôt être protégé par le droit à l'oubli, tantôt, ne pas l'être.

Une seconde différence rend l'assimilation contestable. Pour être protégés par le droit au respect de la vie privée, un fait, une donnée devraient effectivement relever de la vie privée. La sanction de l'auteur d'une divulgation n'est donc envisageable que si l'on peut considérer que l'information relève de la vie privée de la personne.

Au-delà du fait que cette approche réduit considérablement le champ d'application potentiel d'un droit à l'oubli, la détermination du caractère public ou privé de l'information divulguée génère des difficultés particulières. On doit notamment se demander si la première diffusion d'une information dans la presse ou sur Internet épuise le droit à la vie privée ? Autrement dit, a-t-elle pour effet de purger définitivement le caractère privé des faits ? La jurisprudence est partagée[47].

En pratique, les premières décisions ayant eu à se prononcer sur l'existence d'un droit à l'oubli avaient trait à l'opposition de personnes concernées par des affaires judiciaires à la relation des faits plusieurs années après qu'ils se soient déroulés.

Le retentissement médiatique d'une affaire, à l'époque des faits, peut avoir une incidence sur le traitement juridique de l'exploitation de ce fait par le biais d'un article de presse ou encore d'une fiction du réel (ou docufiction). Il s'agit là en effet d'un mode de divulgation d'informations qui soulève un contentieux assez récurrent, divulgation à laquelle des personnes s'opposent en invoquant un droit à l'oubli. Il semblerait que dès lors qu'un fait divers a connu

[47] Pour une réponse négative Cass. 2è 24 nov. 1975, D. 1976 somm. 36 : Il existe un pouvoir discrétionnaire de s'opposer à une re-divulgation de faits privés. Pour une réponse positive : CA Paris 13 mars 1986 D. 1986 IR 445 obs. Lindon, éléments connus de la vie de Y. Noah.

un grand retentissement médiatique, la liberté d'expression autorise à s'en inspirer pour en faire une œuvre de fiction et la liberté d'information, pour en faire un article de presse. Dans ce domaine, la Cour de cassation semble faire la distinction suivante : ou bien les faits ont été suffisamment divulgués pour être considérés comme publics, auquel cas, la rediffusion ne porte plus atteinte à la vie privée et fait obstacle à un droit à l'oubli[48] ; ou bien les faits ont été révélés par l'intéressé lui-même et après avoir soutenu le contraire autrefois, cette circonstance ne doit pas entrer en ligne de compte : la re-divulgation cristallise alors une nouvelle atteinte à la vie privée[49]. Cette distinction n'est cependant pas toujours suivie au fond. La divulgation par l'intéressé peut également être perçue comme un fait justificatif.

De même, l'écoulement du temps peut ramener un fait public dans la sphère privée[50]. Naturellement, la question qui se pose immanquablement est de savoir au bout de combien de temps un fait public est réputé retourner dans la sphère privée. En l'état actuel du droit positif, il est impossible de donner un ordre temporel. On pourrait songer à faire un rapprochement avec le temps juridique, autrement dit, la prescription[51]. Il n'est pas certain, cependant nous l'avons souligné, que le temps de la prescription soit celui de l'oubli. Il est donc très difficile de faire la part des choses et de trouver un critère solide. Les solutions sont très souvent factuelles et le dénouement déprendra très étroitement des circonstances de l'affaire initiale et de sa rediffusion.

La forme de l'information peut également entrer en ligne de compte. Dans les espèces où était en cause l'exploitation journalistique d'affaires judiciaires, c'est la diffusion des images qui était souvent contestée. Il est vrai que l'intérêt légitime de reproduire des images après plusieurs années est parfois contestable. Les images marquent davantage que les écrits et leur reproduction semble porter une atteinte excessive à la personne visée[52]. Mais l'image est-elle couverte par le droit au respect de la vie privée ? *A priori*, elle ne révèle pas forcément la vie privée de la personne. Elle peut simplement révéler une apparence physique. Le droit à l'image au sens strict entre-t-il alors dans le champ de l'article 8 de la CEDH ? Certains soulignent que « la vie privée est pour la CEDH une notion large, couvrant l'intégrité morale (et physique) de la personne, ce qui permet d'inclure le droit à l'image, même lorsque la vie privée *stricto sensu*

[48] Cass. 2ème civ. 22 mai 1996, JCP 1996, IV, 1571. Civ. 1ère 30 mai 2000, CCE 200, 801, obs. A. Lepage ; 3 avril 2002 D. 2002, D2002, jur. 3164, note Bigot et 2003, somm. 1543, obs. Caron ; Cass. 2ème civ. 3 juin 2004.
[49] T. Hassler, « Droit de la personnalité : Rediffusion et droit à l'oubli », D. 2007, p. 2829, §8. – V. aussi Cass. 2ème civ., 14 nov. 1975, D. 1976, jur 241, note B. Edelman ; Cass. 1ère civ., 20 nov. 1990 ; Cass. 1ère civ. 30 mai 2000, D. 2001, somm. 1989 obs. Marino.
[50] C. caron, « A propos du conflit entre les œuvres de fiction et la vie privée », D. 2003, p. 1715.
[51] V. *supra*, développements sur la prescription.
[52] I. Paulik, « Liberté d'expression par l'image et respect des droits de la personnalité », Petites affiches, 2004, p. 14 ; Voir J. Ravanas, « Nécessité de trouver le juste équilibre entre la liberté de l'information et le droit de chacun au respect de sa vie privée », JCP G. 2003, II 10085, commentaire sous cass. 1ère civ. 23 avril 2003.

n'est pas concernée »[53]. Pour autant, la CEDH semble avoir exprimé un avis contraire dans un arrêt en date du 11 janvier 2000 en refusant de sanctionner la publication de photographies ne révélant rien de la vie privée de la personne représentée.

Même lorsque les éléments constitutifs du droit au respect de la vie privée sont réunis, sa mise en œuvre peut naturellement se heurter à certaines limites. Il est évidemment nécessaire de se demander si l'information livrée ou accessible au public satisfait un intérêt légitime, si elle présente une utilité sociale et si elle n'inflige pas à la personne mise en cause ou simplement concernée, une souffrance disproportionnée.

Si l'on ramène cette question à la problématique de la publication d'une image de la personne, on pourrait admettre que prime la liberté d'expression dès lors que la photo publiée ou diffusée poursuit une finalité informative[54]. Il faut que cela aide à la compréhension du propos. La terreur sur les visages des victimes d'attentats permet de mesurer l'ampleur d'un événement dramatique. En revanche, la publication par Paris Match, de la photo de la petite fille assassinée, dans l'affaire dite du pull-over rouge, comme accroche pour l'article à paraître la semaine suivante semble dépourvue de caractère informatif en relation avec le thème abordé. Quant aux informations écrites, se pose la question de l'anonymat. Il paraît normal de pouvoir exiger que le nom des protagonistes ne soit pas reproduit[55].

A l'instar de la liberté d'expression dont il est le pendant, le droit de création, peut également justifier l'utilisation de faits réels ou la divulgation de données personnelles par des tiers. Naturellement, pareil droit n'est pas sans limite et doit être circonscrit. C'est dans le contexte du contentieux de presse et des fictions du réel que l'opposition droit de création et droit à l'oubli – sous couvert de droit au respect de la vie privée – s'est illustrée. Selon la jurisprudence, la liberté de création permet de s'appuyer sur des faits réels à condition que l'évocation de ces faits ne permette pas la révélation d'éléments de la vie privée de la personne concernée qui n'auraient pas été dévoilés[56]. Lorsqu'une fiction s'inspire de faits réels mais s'en détache suffisamment pour que le public ne fasse pas l'amalgame, il n'en résulte pas de préjudice. La difficulté résulte des fictions du réel, qui mêlant la fiction à la réalité, créent la

[53] I. Paulik, « Liberté d'expression par l'image et respect des droits de la personnalité », Petites affiches, 2004, p. 14 citant C. Ruet, l'expression par l'image au regard de l'article 10 de la CEDH, in Image et droit, sous la direction de P. Bloch, l'Harmattan 2002, p. 33 et s.n°33, p. 80.

[54] I. Paulik, « Liberté d'expression par l'image et respect des droits de la personnalité », Petites affiches, 2004, p. 14.

[55] Nous y reviendrons au sujet des données judiciaires notamment.

[56] Cette limite apparaît très nettement dans l'Affaire Francis Heaulme suite à la diffusion du téléfilm intitulé « Dans la tête d'un tueur ». Le juge considère ici que le film porte atteinte au droit au respect de la vie privé, à l'image, au nom et à la présomption d'innocence en présentant Francis Heaulme comme l'auteur d'un double meurtre non élucidé. Seule est retenue l'atteinte à la présomption d'innocence (les autres atteintes sont appréciées conformément aux autres décisions judiciaires), TGI Nanterre, réf., 9 mars 2005, Comm. com. électr. 2005, Comm. 161, A. Lepage ; JCP G 2005, II, 10094, note E. Derieux.

confusion dans l'esprit du public[57]. La cour de cassation a pu sanctionner le fait que les éléments de fiction portent atteinte à la personne dont la fiction s'inspirait car elle lui prêtait des actions et des comportements qu'elle n'avait pas eus[58]. Quelle est la marge de manœuvre dont disposent les auteurs de films s'inspirant de faits réels ? C'est très largement une question d'interprétation[59]. C'est au juge de trancher au cas par cas. Entre la liberté d'expression et de création, d'une part, et le droit au respect de la vie privée, d'autre part, principes d'égale valeur normative, l'équilibre réside dans « la solution la plus protectrice de l'intérêt le plus légitime »[60] mais la jurisprudence demeure très attachée au principe de la liberté d'expression qui l'emporte presque systématiquement. Ainsi, la Cour d'appel de paris soulignait que lorsque « les faits criminels, leur contexte, et la personnalité du demandeur ont été licitement révélés au public par les comptes rendus judiciaires (…), en droit, la relation de faits publics déjà divulgués ne peut constituer en elle-même une atteinte au respect dû à la vie privée ». Le demandeur ayant fait valoir le droit à l'oubli, la Cour ajoute que ce droit « n'a aucune reconnaissance légale et ne saurait prévaloir sur le droit du public à l'information exhaustive et objective »[61].

Si le rattachement du droit à l'oubli au droit au respect de la vie privée nous semble réducteur et pas toujours approprié dans les hypothèses classiques où la jurisprudence y a initialement eu recours, il nous semble encore moins pertinent dans le contexte actuel du numérique. L'exigence de qualification d'éléments de la vie privé est insuffisamment protectrice des individus. Les fournisseurs de services de réseautage social (SRS) par exemple recueillent des informations qui relèvent initialement de la vie privée de la personne mais qui, lorsqu'elles sont partagées, sont traitées comme toute autre information que l'on décide de rendre publique. Ainsi, même si l'information est propre à l'utilisateur, il n'a plus le monopole de son utilisation et son contrôle peut lui échapper. En effet, dès lors qu'une donnée privée est considérée comme « publique », les administrateurs du réseau social ou du moteur de recherche, leurs filiales, partenaires, clients publicitaires ou encore d'autres tiers sont susceptibles de les utiliser. On peut noter que Facebook développe expressément cette notion « *d'information publique* », à l'origine privée. Le fournisseur de réseau social précise qu'il s'agirait d'un

[57] Voir C. Caron, « A propos du conflit entre les œuvres de fiction et la vie privée », D. 2003, p. 1715, qui considère au sujet de fictions reprenant des faits réels, que pour concilier les droits des uns et des autres, « il convient d'encourager les auteurs à maquiller suffisamment les personnages et les circonstances du drame en faisant prévaloir la fiction sur la réalité. Et s'ils souhaitent demeurer fidèles à la réalité, il leur appartient alors de demander l'autorisation de la personne concernée à l'époque par ce fait divers ». Voir également A. Fourlon, « *Toute ressemblance avec des personnages existant ou ayant existé…* » est-elle constitutive d'une atteinte aux droits de la personnalité ? » Comm. com. électr. 2007, étude 5.

[58] Cass. 1ère civ. 7 fév. 2006, n°04-10.941 JCP 2006, II, 10041 note G. Loiseau.

[59] A titre d'exemple, il est possible qu'une personne se reconnaisse dans une fiction du réel mais que des personnes extérieures à l'affaire ne l'identifient pas, V. en ce sens, S. Berland et P.E. Dumora, Gaz. Pal. 2004, n° 130, p. 46.

[60] TGI de Nancy, 9è ch. Civ., ord. de référé, 3 oct. 2006, affaire du petit Grégory, A. Fourlon, préc.

[61] Voir également au sujet du docu-fiction *Virée criminelle*, CA Paris, pôle 2, 7e ch., 26 févr. 2014, n° 13/01241, T. E. B. et a. c/ SA Capa Presse et a., inédit. Comm. com. électr. 2014, chron. 6, obs. B. Montels.

« contenu public pouvant être vu par des personnes qui ne font pas partie de la liste d'amis/contacts du membre, des personnes non connectées ou utilisant d'autres médias (nouveaux ou anciens) comme les supports imprimés, la diffusion (télévision…) et d'autres sites Internet »[62]. Sur ce même réseau, il est intéressant de noter que lorsqu'une personne partage des informations concernant un autre membre, elle peut choisir de les rendre publiques, bien que ce membre ait lui-même choisi de les rendre visibles à un public réduit sur son propre profil. Enfin, certaines informations sont considérées comme toujours publiques, telles que le nom, les photos de profil et de couverture, les réseaux utilisés, le sexe, le nom d'utilisateur et l'identifiant. De même, certains contenus des groupes LinkedIn, réseau social professionnel, peuvent être publics et consultables sur Internet si le propriétaire du groupe a ouvert celui-ci aux discussions publiques.[63]

Dans ce contexte, on peut penser que « la vie privée est devenue un concept sans pertinence »[64] notamment parce qu'elle ne règle qu'une fraction des problématiques soulevées par le droit à l'oubli. « Sur Internet, il y a des activités publiques tandis que d'autres supposent un certain nombre d'intérêts relatifs à la vie privée. Pour fonder une approche conforme à l'impératif d'équilibre entre l'ensemble des droits fondamentaux, il faut tenir compte de l'aspect en continuum des situations publiques et des situations privées. Dans le cyberespace, tout n'est pas que public ou que privé comme s'il n'y avait que le noir et le blanc. L'intensité publique et privée des situations est en nuances variables selon les contextes et les circonstances »[65]. C'est ce qui explique l'intérêt qu'il a à réexplorer le dispositif de protection des données à caractère personnel.

2.3. Droit à l'oubli et protection des données à caractère personnel

En 1978, le législateur français s'engageait dans la protection des données à caractère personnel. A l'époque, dans la ligne de mire, principalement, les fichiers des administrations publiques[66], ceux là-même qui, selon l'enquête sociologique, suscitent le moins d'inquiétude. Les instances européennes s'emparent de la question et, en 1995, proposent un dispositif dont l'un des avantages tient à son rayonnement territorial. Il s'articule avec d'autres, et l'on songe

[62]Rubrique « informations publiques » - politique de confidentialité Facebook
[63]Article 2.10. « Groupes » – politique de confidentialité LinkedIn
[64] A. Bensoussan, in J.P. Sueur, *Numérique, renseignement et vie privée : de nouveaux défis pour le droit,* Rapport d'information sénat, n° 666, 27 juin 2014, p. 57.
[65] P. Trudel, « Quelles limites à la googleisation des personnes ? » *in La sécurité de l'individu numérisé, Réflexions prospectives et internationales*, S. Lacour (dir.), L'Harmattan 2010, p.52.
[66] E. Derieux, « Protection des données personnelles et communication au public en ligne, Loi du 6 juillet 1978 relative à l'informatique, aux fichiers et aux libertés et autres textes », Revue Lamy Droit de l'immatériel 2011, n° 68.

notamment au dispositif mis en place par la directive européenne n° 2000/31 du 8 juin 2000, relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (directive sur le commerce électronique), dont la section 4 est consacrée à « la responsabilité des prestataires intermédiaires ». En effet, face à l'accroissement considérable des conflits mettant en cause les fournisseurs intermédiaires d'Internet, notamment les hébergeurs, pour obtenir la suppression de contenus illicites diffusés sur Internet, le législateur européen a souhaité harmoniser les dispositions gouvernant la responsabilité des intermédiaires. Transposant la directive, le législateur français, par une loi n° 2000-719 du 1er août 2000, modifiant la loi n° 86-1067 du 30 septembre 1986, relative à la liberté de communication, adoptait des principes de responsabilité applicables aux fournisseurs Internet. Les principales dispositions de ce texte ont fait l'objet d'une nouvelle modification avec l'adoption de la loi n° 2004-575 du 21 juin 2004, pour la confiance dans l'économie numérique et le droit de la communication, dite LCEN, sur laquelle nous reviendrons ultérieurement[67].

La révolution numérique de ces dernières années a néanmoins conduit les instances européennes à engager un processus de rénovation du régime de protection des données à caractère personnel. Le dispositif présent, et probablement à venir, vise à protéger les données à caractère personnel et entend en règlementer le traitement. Le droit à l'oubli n'est pas expressément consacré dans la directive de 1995 et ne l'est plus dans la proposition de règlement du 25 janvier 2012, amendée par la résolution du 12 mars 2014 mais il est latent dans un certain nombre de dispositions phares, notamment celles qui posent le principe d'un droit d'accès, d'un droit de rectification et d'un droit d'opposition au traitement des données à caractère personnel (2.2.1). De manière plus générale, il étaye également la règlementation des durées de conservation des données qui présente un lien ténu avec le droit à l'effacement (2.2.2).

2.3.1. Droit à l'oubli et droit d'accès, droit à rectification et droit d'opposition

L'appel à projet de la mission de recherche Droit et justice soulignait que « la loi informatique et libertés confère d'ores et déjà aux personnes dont des données personnelles sont collectées et enregistrées des droits de suppression et de rectification de ces données » et regrettait que, « en dépit de l'existence de ces droits, certaines données ne sont pas

[67] La proposition de règlement de 2012 sur la protection des données affirme la volonté de concilier les deux dispositifs, l'article 1 §3 disposant : « Le présent règlement s'applique sans préjudice de la directive 2000/31/CE, et en particulier des dispositions des articles 12 à 15 de ladite directive établissant les règles en matière de responsabilité des prestataires intermédiaires ».

définitivement effacées et peuvent resurgir à tout moment ». En d'autres termes, il est considéré qu'en l'état actuel des textes, le droit à l'oubli ne peut véritablement être assuré. Qu'en est-il exactement ? A la lecture de l'article 1er et du considérant 10 de la directive 95/46, il apparaît que le dispositif de protection des données à caractère personnel vise à garantir un niveau élevé de protection des libertés et des droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel[68].

Le considérant 25 de la directive 95/46 précise d'ailleurs que les principes de la protection prévus par celle-ci trouvent leur expression, d'une part, dans les obligations mises à la charge des personnes qui traitent des données, ces obligations concernant en particulier la qualité des données, la sécurité technique, la notification à l'autorité de contrôle, les circonstances dans lesquelles le traitement peut être effectué, et, d'autre part, dans les droits conférés aux personnes dont les données font l'objet d'un traitement d'être informées sur celui-ci, de pouvoir accéder aux données, de pouvoir demander leur rectification, voire de s'opposer au traitement dans certaines circonstances.

La Cour de justice de l'Union européenne a clairement énoncé dans plusieurs décisions que les dispositions de la directive 95/46, en ce qu'elles régissent le traitement de données à caractère personnel susceptibles de porter atteinte aux libertés fondamentales et, en particulier, au droit à la vie privée, doivent nécessairement être interprétées à la lumière des droits fondamentaux qui, selon une jurisprudence constante, font partie intégrante des principes généraux du droit dont la Cour assure le respect et qui sont désormais inscrits dans la Charte des droits fondamentaux de l'Union européenne[69].

Ainsi, l'article 7 de la Charte garantit le droit au respect de la vie privée, tandis que l'article 8 de la Charte proclame expressément le droit à la protection des données à caractère personnel. Les paragraphes 2 et 3 de ce dernier article précisent d'abord que ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi, ensuite, que toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification et, enfin, que le respect de ces règles est soumis au contrôle d'une autorité indépendante. Ces exigences sont mises en œuvre notamment par les articles 6, 7, 12, 14 et 28 de la directive 95/46.

[68] Voir, en ce sens, arrêt IPI, aff. C-473/12, 7 nov. 2013, point 28.
[69] Déclaration des droits adoptée le 7 décembre 2000 par l'Union européenne. Voir arrêt Connolly/Commission, aff.C-274/99, 6 mars 2001, point 37 ; également, arrêt Österreichischer Rundfunk e.a., aff. 465/00, 20 mai 2003 pont 68.

En droit interne, dans une section 2, intitulé : « Droits des personnes à l'égard des traitements de données à caractère personnel », la loi informatique et liberté de 1978 instaure tout d'abord, un **droit d'opposition** permettant à toute personne physique de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement[70] sauf lorsque le traitement répond à une obligation légale ou en cas de renonciation dans l'acte autorisant le traitement[71]. Elle est en droit de s'opposer, sans frais, à ce que les données la concernant soient utilisées à des fins de prospection, notamment commerciale, par le responsable actuel du traitement ou celui d'un traitement ultérieur. Ainsi, une personne devrait pouvoir se prévaloir du droit d'opposition à l'encontre d'un éditeur de site Internet ou d'un fournisseur de services de réseautage social par exemple, lorsqu'il exploite à des fins commerciales les données à caractère personnel la concernant. Concrètement, il s'agit par exemple de s'opposer à ce que l'opérateur établisse des profils de ses clients ou membres à des fins de prospection commerciale, pour son compte ou pour le compte d'un tiers. L'article 17 §1 c) de la proposition de règlement fait une référence explicite à l'article 19 qui reprend le droit d'opposition institué par l'article 38 de la loi informatique et libertés. L'article 19 §2 de la proposition de la Commission réservait un droit d'opposition au cas où les données à caractère personnel étaient traitées à des fins de *marketing direct* ». La résolution du Parlement ne reprend pas cette finalité spécifique. Elle est comprise dans le droit d'opposition en général dont la résolution parlementaire entend faciliter la mise en œuvre.

La loi institue, ensuite, à l'article 39 un **droit d'accès** permettant à toute personne physique justifiant de son identité d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir toutes informations utiles sur le traitement des données la concernant. Elle peut ainsi obtenir :

« 1° La confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement ;

2° Des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées ;

3° Le cas échéant, des informations relatives aux transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne ;

4° La communication, sous une forme accessible, des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ;

[70] Article 38 al. 1.
[71] Article 38 al. 2.

5° Les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé ».

Ce droit n'est pas absolu et la loi offre au responsable du traitement la possibilité de s'opposer aux demandes manifestement abusives, notamment par leur nombre, leur caractère répétitif ou systématique.

En outre, ces mesures ne s'appliquent pas lorsque les données à caractère personnel sont conservées sous une forme excluant manifestement tout risque d'atteinte à la vie privée des personnes concernées et pendant une durée n'excédant pas celle nécessaire aux seules finalités d'établissement de statistiques ou de recherche scientifique ou historique (art. 39-II).

La loi de 1978 offre enfin, à l'article 40, un **droit à rectification** – allant jusqu'à l'effacement – à toute personne physique justifiant de son identité destiné à lui permettre d'obtenir du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite.

Dans l'hypothèse où une donnée a été transmise à un tiers, le responsable du traitement doit accomplir les diligences utiles afin de lui notifier les opérations qu'il a effectuées conformément au premier alinéa.

Les héritiers d'une personne décédée justifiant de leur identité peuvent, si des éléments portés à leur connaissance leur laissent présumer que les données à caractère personnel la concernant faisant l'objet d'un traitement n'ont pas été actualisées, exiger du responsable de ce traitement qu'il prenne en considération le décès et procède aux mises à jour qui doivent en être la conséquence.

Lorsque la personne concernée ou ses héritiers en font la demande, le responsable du traitement doit justifier qu'il a procédé aux opérations requises.

Ces dispositions exposées succinctement ne comportent pas de trace directe du droit à l'oubli mais elles l'induisent nécessairement. Les données effacées suite au retrait, à l'opposition ou à la rectification finissent par être oubliées car c'est là le rôle normal de la mémoire humaine que de procéder à un tri des informations à retenir. Non aidé par un support matériel, papier ou numérique, le cerveau humain élimine certaines informations non essentielles. Ces dispositions ont néanmoins, un temps, été jugées insuffisantes pour protéger les droits fondamentaux de la personne. C'est la raison pour laquelle les instances européennes

avaient décidé d'intituler l'article 17 de la proposition de règlement du 25 janvier 2012 « le droit à l'oubli et à l'effacement », un article inséré dans une section 3 concernant la rectification et l'effacement. Celle-ci fait partie du chapitre relatif au droit des personnes.

Le symbole était fort mais restait il est vrai, à ce simple degré de symbole puisque le corps de ce même article ne faisait plus aucune référence au droit à l'oubli. C'est peut-être ce qui explique l'amendement effectué par la résolution du 12 mars 2014 qui, conformément au souhait exprimé par la commission LIBE[72], a éliminé la référence explicite à un droit à l'oubli. Dans sa dernière version, le titre de l'article 17 devient « le droit à l'effacement ». L'amendement signe-t-il l'arrêt de mort du droit à l'oubli ? Difficile de l'affirmer de façon péremptoire.

L'apparition d'un droit à l'oubli dans la proposition initiale de règlement pouvait sans doute réjouir les partisans de ce droit mais même dans cette première version, il était permis de se demander si le contenu de l'article 17 permettait réellement la construction d'un droit à l'oubli. Au fond, à y regarder de plus près, il apparaît que le contenu des versions successives de règlement offre les mêmes prérogatives qu'auparavant : droit d'accès, droit à rectification pouvant aller jusqu'à l'effacement et droit d'opposition au traitement des données à caractère personnel.

Le rapport LIBE fournit une justification à la position finalement retenue dans la résolution : « Le droit à l'effacement et le droit à la rectification sont importants pour les personnes concernées car de plus en plus d'informations sont diffusées, ce qui peut être lourd de conséquences. Néanmoins, si une publication de données à caractère personnel était fondée sur des motifs juridiques tels que visés à l'article 6, paragraphe 1 (définissant les cas de traitements licites), un droit à l'oubli numérique ne serait ni réaliste ni légitime (Voir l'amendement connexe à l'article 17, paragraphe 2 bis, et au considérant 54). Cela n'implique pas que des tiers soient autorisés à réutiliser des données à caractère personnel ayant été publiées sans disposer de motif juridique valable ».

La lecture des considérants 53 et 54 de la proposition de règlement est à cet égard très révélatrice de la volonté de demeurer dans le cadre tracé par les textes antérieurs : « Toute personne devrait avoir le droit de faire rectifier des données à caractère personnel la concernant, et disposer d'un droit à l'effacement lorsque la conservation de ces données n'est pas conforme au présent règlement. En particulier, les personnes concernées devraient avoir le droit d'obtenir que leurs données soient effacées et ne soient plus traitées, lorsque ces données ne sont plus

[72] Rapport du 21 octobre 2013 de la Commission des libertés civiles, de la justice et des affaires intérieures (LIBE), A7-0403/2013.

nécessaires au regard des finalités pour lesquelles elles ont été recueillies ou traitées, lorsque les personnes concernées ont retiré leur consentement au traitement ou lorsqu'elles s'opposent au traitement de données à caractère personnel les concernant ou encore, lorsque le traitement de leurs données à caractère personnel n'est pas conforme au présent règlement.

Toutefois, la conservation des données devrait être autorisée lorsqu'elle est nécessaire à des fins statistiques ou de recherche historique ou scientifique, pour des motifs d'intérêt général dans le domaine de la santé publique, ou à l'exercice du droit à la liberté d'expression, si elle est requise par la loi ou s'il existe une raison de limiter le traitement des données au lieu de les effacer. De la même manière, le droit à l'effacement ne devrait pas s'appliquer lorsque la conservation de données à caractère personnel est nécessaire pour l'exécution d'un contrat avec la personne concernée, ou lorsqu'il existe une obligation juridique de conserver ces données ».

Et le considérant 54 d'ajouter : « Afin de renforcer le "droit à l'effacement" dans l'environnement en ligne, le droit à l'effacement des données devrait en outre être étendu de façon à ce que le responsable du traitement qui a rendu les données à caractère personnel publiques sans motif légal soit tenu de prendre toutes les mesures nécessaires pour procéder à l'effacement de ces données, y compris pas des tiers, sans préjudice du droit de la personne concernée à demander réparation ».

A priori donc, le législateur n'a pas souhaité instituer un droit à l'oubli peut-être parce que l'articulation de certaines prérogatives rend possible un oubli au profit de la personne concernée.

2.3.2. Droit à l'oubli, droit à l'effacement numérique et limitation de la durée de conservation des données personnelles

Alors que les auteurs de la proposition de règlement le voulaient autonome pour en accroître la charge symbolique, le droit à l'oubli vient s'articuler avec le droit à l'effacement (et s'efface désormais à son profit), le principe du consentement, les questions relatives à la durée de conservation, pour ne citer que ces points. Son articulation avec les autres dispositions du projet de règlement (et de la directive toujours en vigueur) n'en est que plus difficile.

Il convient alors de montrer en quoi le droit à l'effacement numérique s'inscrit dans la continuité des dispositions existantes, reprises ou modifiées par le projet de règlement, et s'accorde avec elles, ou dans quelle mesure il constitue une rupture. Notre propos visera en particulier à mettre en évidence les rapports entre droit à l'oubli et durée de conservation des données. Il est à noter à ce stade que le terme même de conservation n'est pas défini et gagnerait à l'être à l'avenir.

L'effacement sera présenté d'abord comme un corollaire de la limitation de la durée de conservation avant d'être examiné comme un motif d'interruption de cette durée. La conservation (sans limites) sera présentée enfin comme une limite au droit à l'effacement.

2.3.2.1. L'extinction de la durée de conservation, déclencheur du droit à l'effacement

L'effacement qui est une composante du droit d'accès est aussi une conséquence de la durée de conservation des données.

2.3.2.1.1. L'effacement, composante du droit d'accès

Composante du droit d'accès, le droit à l'effacement se présente dans la directive de 1995 comme un remède à la non-conformité des traitements, sa vertu étant donc surtout curative.

L'article 12 de la directive organisant le droit d'accès prévoit ainsi : « Les États membres garantissent à toute personne concernée le droit d'obtenir du responsable du traitement:

a) sans contrainte, à des intervalles raisonnables et sans délais ou frais excessifs:

- la confirmation que des données la concernant sont ou ne sont pas traitées, ainsi que des informations portant au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte et les destinataires ou les catégories de destinataires auxquels les données sont communiquées,

- la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine des données,

- la connaissance de la logique qui sous-tend tout traitement automatisé des données la concernant, au moins dans le cas des décisions automatisées visées à l'article 15 paragraphe 1;

b) selon le cas, la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la présente directive, notamment en raison du caractère incomplet ou inexact des données;

c) la notification aux tiers auxquels les données ont été communiquées de toute rectification, tout effacement ou tout verrouillage effectué conformément au point b), si cela ne s'avère pas impossible ou ne suppose pas un effort disproportionné ».

Ce motif subsiste dans la proposition de règlement mais n'est qu'un de ceux que la personne peut invoquer à l'appui de sa demande d'effacement et de cessation de la diffusion des données. Il se différencie des autres et nouveaux motifs qui s'inscrivent dans la perspective

d'un contrôle croissant du parcours de ses données par la personne concernée par les traitements. S'il n'est pas surprenant que la personne puisse demander l'effacement à l'appui d'une opposition au traitement de ses données, l'interprétation des autres motifs soulève plus de difficultés.

2.3.2.1.2. L'effacement, conséquence de la limitation de la durée de conservation

Composante du droit d'accès, le droit à l'effacement devient aussi une composante du principe de limitation de la durée de conservation des données personnelles qui fait partie des principes essentiels du dispositif juridique de protection des données. En effet, il est désormais expressément prévu dans la proposition de règlement que le droit d'obtenir l'effacement puisse être exercé à l'expiration du délai de conservation.

Pour logique qu'elle paraisse, cette disposition souligne le flou qui entourait jusqu'alors le sort des données arrivées à terme. En dehors d'un effacement, quel pouvait être le sens et la concrétisation de la fixation d'un délai pour la conservation ? Contrairement à ce que l'on peut penser, des hypothèses de prolongation de la durée de conservation existent, dans le cas par exemple où le contrôle des données change de main et passe du responsable vers la personne concernée qui en a la garde à partir d'un certain moment. C'est une solution qui a été préconisée dans un projet visant à traiter des données physiologiques pour pouvoir porter assistance à des personnels en danger (les pompiers par exemple)[73]. L'intérêt du changement de main réside dans la possibilité pour le salarié de bénéficier des données traitées pour une première finalité afin d'en atteindre une seconde (l'amélioration de la santé) dans une optique de *quantified self*.

Les nouvelles dispositions relatives à l'effacement privilégient en tout cas l'oubli de soi et dans le même temps l'oubli par le responsable de traitement. Il existe cependant une alternative qui n'est pas évoquée dans le texte et qui représente un enjeu majeur pour l'économie numérique et pour le marché dit de la confiance. Il s'agit de la rétrocession des données à la personne concernée, qui par son travail gratuit, fournit un ensemble d'informations qui représente pour les entreprises du secteur un nouvel or noir. Ce n'est pas ici la question d'un droit propriété des personnes sur leurs données qui est posée, et qui peut être un facteur bloquant, mais bien celle de l'appropriation du surplus de l'exploitation réalisée par les organismes quels qu'ils soient.

[73] A. Blandin, E. Juet, « La prévention des risques professionnels à la lumière de la loi informatiques et libertés : le cas du dispositif S_Pod », colloque *Innovations technologiques dans le contexte professionnel*, MSHB, 26 et 27 juin 2014.

Le rapport Colin et Collin sur la fiscalité du numérique consacre un important développement à cette question, alimenté presque exclusivement par des travaux anglo-saxons[74]. Sont évoquées en particulier, « les applications inspirant à ses utilisateurs une activité, dont les externalités positives vont, sous la forme de données, s'incorporer à la chaîne de production sans contrepartie monétaire ». Le droit à la protection des données personnelles est alors présenté comme un rempart contre ce qui s'apparente à une véritable prédation des données par les entreprises.

La restitution est d'ores et déjà pratiquée dans certains pays et notamment en France où elle fait par exemple l'objet d'une expérimentation menée par la Fondation Internet nouvelle génération (FING). Intitulée http://fing.org/?MesInfos-quand-les-donnees, cette expérimentation s'appuie sur une démarche volontaire de plusieurs entreprises qui acceptent de partager les données plutôt que de s'en dessaisir au demeurant. « L'idée de regrouper plusieurs grandes organisations qui "couvrent" une part importante des pratiques quotidiennes des individus est essentielle : une entreprise isolée qui choisirait de partager ses données avec ses clients n'en apprendrait pas grand-chose, parce que la valeur de chaque donnée augmente de manière exponentielle à mesure que l'individu approche d'une vision "à 360°" de sa propre vie ».

Ces initiatives ne répondent pas en priorité à un souci d'amélioration du contrôle que les personnes peuvent exercer sur leurs données. Elles s'inscrivent davantage dans la perspective de valorisation des données et d'amélioration de la confiance.

Si on les rapporte au nouvel article sur le droit à l'effacement, force est de constater qu'elles peinent à s'articuler avec lui. A supposer que la restitution soit une alternative à l'effacement, la négociation avec le responsable du traitement devient indispensable. Mais elle pourrait s'avérer difficile car les dispositions actuelles opposent davantage les responsables et les individus qu'elles ne les incitent à coopérer. L'enquête sociologique révèle en tous les cas que les usagers ne perçoivent par la collecte de leurs données à caractère personnel de cette façon. C'est toute la conception personnaliste du droit à la protection des données personnelles qui trouve ici ses limites car elle isole l'individu protégé, là où certains usages plaident en faveur d'une coopération entre les différents acteurs.

[74] P. Collin et N. Colin, *Mission d'expertise sur la fiscalité du numérique*, Rapport au Ministre de l'économie et des finances, au Ministre du redressement productif, au Ministre chargé du budget, à la Ministre déléguée chargée des petites et moyennes entreprises, de l'innovation et de l'économie numérique, janvier 2013.

Pour revenir à des pratiques plus communes et toujours pour montrer qu'extinction du délai ne signifie pas effacement automatique, notons que l'archivage constitue une autre modalité de vie de la donnée après la fin de la période de conservation si l'on se réfère aux textes de la CNIL, notamment les déclarations simplifiées comme celle concernant les traitements relatifs à la gestion de clients et de prospects (norme simplifiée n° 48).

Pourtant dans d'autres cas, l'archivage est assimilé à la conservation et ne constitue pas une modalité qui intervient à l'issue du délai de conservation. La durée de conservation en deux temps prévue par le dispositif PNR[75] (données actives puis passives) ne distingue pas en effet conservation d'abord puis archivage.

Des alternatives à l'effacement sont aussi prévues dans la proposition de règlement. Dans certains cas, une limitation du traitement peut se substituer à l'effacement. Quatre cas sont envisagés :

- a) pendant une durée permettant au responsable du traitement de vérifier l'exactitude des données lorsque cette dernière est contestée par la personne concernée;
- b) lorsqu'elles ne sont plus utiles au responsable du traitement pour qu'il s'acquitte de sa mission, mais qu'elles doivent être conservées à des fins probatoires, ou
- c) lorsque leur traitement est illicite et que la personne concernée s'oppose à leur effacement et exige à la place la limitation de leur utilisation;
- d) lorsque la personne concernée demande le transfert des données à caractère personnel à un autre système de traitement automatisé, conformément à l'article 18, paragraphe 2.

Toutefois, dans certains textes, l'effacement est prévu explicitement comme une conséquence de l'extinction de la durée de conservation. En reprenant l'exemple de la norme n° 48, on note que l'effacement est prévu mais que l'archivage est une alternative. Il est important de souligner que l'effacement apparaît alors comme une obligation pour le responsable et non comme un droit que peut invoquer la personne concernée. Une telle approche est de nature à favoriser un effacement effectif et par conséquent un oubli car l'usager n'a pas à en faire explicitement la demande, démarche jugée complexe pour bon nombre d'entre eux.

En tous les cas, en liant droit à l'effacement et durée de conservation, on amplifie les difficultés que suscite le choix de la durée de conservation proportionnée à la finalité poursuivie.

[75] Accord *Passenger Name Record* passé entre l'Union européenne et les États-Unis sur les données des passagers aériens.

2.3.2.2. La subordination du droit à l'effacement à des durées de conservation disparates

Le débat sur le droit à l'oubli est ainsi l'occasion de découvrir toute l'importance de la durée de conservation. Une prise de conscience s'opère et l'on mesure à quel point les durées de conservation des données sont très variables pour une même finalité, tout comme les fondements de la détermination de cette durée (décision du responsable du traitement, recommandations, prescriptions légales…). Certains semblent même s'émouvoir qu'une durée de conservation limitée puisse exister lorsqu'ils évoquent un risque d'amnésie collective en cas de mise en œuvre d'un éventuel droit à l'oubli.

2.3.2.2.1. – Des durées disparates

Avant de s'intéresser à la disparité des durées de conservation, il convient de mettre l'accent sur la diversité des instruments juridiques qui les déterminent. Le responsable du traitement peut être amené à fixer librement la durée sous réserve qu'elle soit proportionnée à la finalité du traitement. Dans certains cas, les autorités de régulation interviennent pour recommander une durée qu'elles estiment être proportionnée. A cela s'ajoute l'ensemble du dispositif légal qui fixe des durées de conservation.

Dans ce domaine, une évolution mérite d'être signalée, c'est celle qui consiste à fixer des durées de conservation dans des instruments traitant spécifiquement des données personnelles comme la directive « rétention des données » sur laquelle nous reviendrons. Dans ce cas, c'est l'augmentation de la durée de conservation qui est visée et non la limitation, ce qui est vivement critiqué par ceux qui estiment que la société de surveillance ne connaît plus de limites. Du point de vue juridique, cet allongement constitue une dérogation à la règle et confirme l'existence d'une situation d'exceptionnalité[76].

L'enchevêtrement entre les durées librement déterminées et les durées légales est constant comme le montre encore la norme n° 48. En réalité, l'encadrement de la fixation de la durée est double, par le principe de proportionnalité, d'une part, et par les obligations légales de l'autre.

[76] Sur ce thème, V. M. Goupy, « Etat d'exception », in V. Bourdeau et R. Merrill (dir.), *Dictionnaire de théorie politique,* 2012. http://www.dicopo.fr/spip.php?article131.

En outre, comme l'illustre le cas des données bancaires, la durée de conservation est à concevoir plus comme un processus que comme une limite unique :

« Les données relatives aux cartes bancaires doivent être supprimées une fois la transaction réalisée, c'est-à-dire dès son paiement effectif. Dans le cas d'un paiement par carte bancaire, elles peuvent être conservées pour une finalité de preuve en cas d'éventuelle contestation de la transaction, en archives intermédiaires, pour la durée prévue par l'article L 133-24 du code monétaire et financier, en l'occurrence 13 mois suivant la date de débit. Ce délai peut être étendu à 15 mois afin de prendre en compte la possibilité d'utilisation de cartes de paiement à débit différé.

Ces données peuvent être conservées plus longtemps sous réserve d'obtenir le consentement exprès du client, préalablement informé de l'objectif poursuivi (faciliter le paiement des clients réguliers par exemple). Ce consentement peut être recueilli par l'intermédiaire d'une case à cocher (non précochée par défaut), par exemple et ne peut résulter de l'acceptation de conditions générales.

Les données relatives au cryptogramme visuel ne doivent pas être stockées.

Lorsque la date d'expiration de la carte bancaire est atteinte, les données relatives à celles-ci doivent être supprimées ». [77]

Il arrive que les choix quant à la durée de conservation soient contestés. Dans son avis sur les moteurs de recherche, le Groupe de travail « article 29 »[78] (ci-après G29) avait ainsi préconisé une durée de conservation de 6 mois. Celle-ci n'a pas été respectée par Google qui imposait une durée de 18 mois[79]. C'est à la suite d'une négociation que la durée a été fixée finalement à 12 mois.

Ce type de négociations augmente la disparité des durées et brouille la visibilité du dispositif pour les usagers. Dans une communication sur la gestion de l'information dans le cadre de l'Espace de liberté, de sécurité et de justice, la Commission européenne s'en est inquiétée. Elle distingue plusieurs instruments qui se superposent au fil du temps et se lance dans un exercice de cartographie de l'information pour décrire le modèle européen.

---

[77] Norme n° 48 précit.

[78] Le groupe de travail « article 29 » sur la protection des données a été institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Il a un caractère consultatif et agit en toute indépendance. Ses avis sont souvent pris comme référence, et sont largement relayés par les autorités de protection des données à l'échelle européenne, et notamment par la CNIL.

[79] Avis 1/2008 *sur les aspects de la protection des données liés aux moteurs de recherche du 4 avril 2008*, Groupe de travail « article 29 » sur la protection des données.

Si on ne retient que les instruments qui prévoient une collecte des données personnelles au niveau de l'Union européenne, on en recense déjà six : les instruments visant à améliorer le fonctionnement de l'espace Schengen et de l'union douanière, le système d'information de Schengen, EURODAC (système centralisé et automatisé d'identification des empreintes digitales de certains ressortissants de pays tiers ayant exclusivement pour but de contribuer à déterminer l'État membre responsable, au titre du règlement Dublin, de l'examen d'une demande d'asile), le Système d'information des visas (VIS), le Système d'information douanier (SID). S'ajoute à cela Europol et Eurojust. Ces instruments spécialisés ne sont pas harmonisés de telle sorte que les durées de conservation des données sont extrêmement variables d'un instrument à l'autre (de 24 heures à 15 ans). La disparité est d'une telle ampleur parfois que l'on s'éloigne de toute rationalité.

L'appréciation de la durée réelle de conservation est rendue d'autant plus difficile qu'une distinction est faite parfois entre des bases de données passives et actives. En matière de transferts de données vers les Etats tiers, c'est l'approche que l'on trouve dans le dispositif PNR. Mais une même différenciation s'opère par exemple pour les moteurs de recherche selon que le traitement constitue un référencement, qui rend public le lien vers un contenu, ou une indexation qui demeure un traitement caché et sous le seul contrôle du moteur.

On pourrait multiplier les exemples mais l'essentiel est de s'interroger sur le point de savoir si les durées définies sont proportionnées à l'objectif poursuivi.

2.3.2.2.2. – Des durées disproportionnées

Le contrôle de la durée fait partie des prérogatives des régulateurs.

Dans sa consultation sur le droit à l'oubli en direction des experts, la CNIL proposait ainsi qu'une réflexion soit initiée dans le cadre du G29 pour la définition de ces durées de conservation. Cela pourrait se traduire par l'élaboration d'un document de référence à destination des responsables de traitement.

Avant de déterminer les conditions d'un travail d'harmonisation, il conviendrait de s'interroger sur les conséquences du contrôle renforcé de la personne sur ses données qu'augure l'article 17 de la proposition de règlement. Dès lors que la personne peut demander l'effacement quand elle juge que les données ne sont plus nécessaires au regard de la finalité, dès lors qu'elle peut retirer son consentement, cela ne signifie-t-il pas que la durée peut être interrompue avant

l'expiration du terme ? Cette durée ne devient-elle pas (en dehors des cas de durée obligatoire) un élément négociable au moment où le consentement est donné ?

Si tel est le cas, l'enjeu est d'abord de mieux définir le champ des durées prescrites par la loi ou le règlement et le champ des durées librement définies et consenties, sous réserve d'un encadrement de la liberté contractuelle. Ces réserves étant faites, un référentiel pourrait être établi. L'harmonisation peut porter sur les durées pour une même finalité. Est-ce suffisant toutefois, compte tenu de l'enchevêtrement des données ? Ne devrait-on pas ajouter un critère lié au type de traitement ?

La question de la proportionnalité de la durée de conservation des données a été posée de manière explicite dans le récent arrêt concernant la directive « rétention des données » de 2006.

Cette directive, qui imposait la conservation des données de communications électroniques pour qu'elles soient accessibles aux autorités judiciaires et policières, a été invalidée, solution assez radicale dont l'importance mérite d'être soulignée. La Cour de justice de l'Union européenne a estimé que l'ingérence dans les droits fondamentaux à la vie privée et à la protection des données personnelles était caractérisée, puis elle s'est demandé si cela était justifié. Bien que cette directive poursuive un objectif d'intérêt général, la lutte contre la criminalité grave, la Cour a considéré que le législateur de l'Union avait excédé les limites qu'impose le respect du principe de proportionnalité[80].

En quoi consiste cet excès ? La conservation des données elle-même peut être considérée comme apte à réaliser l'objectif poursuivi par la directive. En revanche, c'est l'absence de règles claires et précises régissant la portée de l'ingérence dans les droits fondamentaux qui est mise en évidence par la Cour.

En ce qui concerne spécifiquement la durée de conservation des données, la Cour indique : « la directive 2006/24 impose, à son article 6, la conservation de celles-ci pendant une période d'au moins six mois sans que soit opérée une quelconque distinction entre les catégories de données prévues à l'article 5 de cette directive en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées. Cette durée se situe, en outre, entre six mois au minimum et vingt-quatre mois au maximum, sans qu'il soit précisé que la

[80] CJUE, 8 avril 2014, aff. jointes C-293/12 et C-594/12, Digital Rights Ireland et Seitlinger e.a.

détermination de la durée de conservation doit être fondée sur des critères objectifs afin de garantir que celle-ci est limitée au strict nécessaire. »

2.3.2.3. L'interruption de la durée de conservation par la demande d'effacement

Deux motifs pouvant être invoqués à l'appui d'une demande d'effacement soulèvent des questions délicates.

D'abord, la proposition de règlement prévoit que la demande d'effacement pourra être faite si la personne estime que ses données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées. Elle devient de ce fait juge de la proportionnalité entre les finalités déclarées et les traitements opérés. Ensuite, le retrait du consentement sur lequel est fondé le traitement pourra être un motif de demande d'effacement.

2.3.2.3.1. – Le droit au retrait, fondement de l'effacement

Le droit au retrait mérite à lui seul un commentaire. Le G29 estime qu'il existait déjà de manière implicite dans la directive de 1995. De manière plus explicite, la directive 2002/58/CE le prévoit pour les données de localisation. Le G29 le présente alors comme une application du droit d'opposition au traitement de données de localisation[81].

Mais le retrait n'a vocation à être exercé qu'à l'égard des traitements futurs et non passés. On considère donc que dans la période passée, les données ont été légitimement collectées *a priori*. Bien entendu, les choses sont différentes si un traitement non conforme est avéré, car dans ce cas la demande d'effacement à titre curatif sera pleinement fondée. Nul besoin alors d'exercer préalablement le droit de retrait.

Mais dans le cas du retrait, c'est le défaut de base juridique à partir du retrait qui empêchera le traitement futur. L'article 7 de la proposition de règlement le confirme : « La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement préalablement donné ».

Or, l'article 17 de la proposition de règlement prévoit que c'est le retrait du consentement qui déclenche l'effacement. Il y a là une logique très différente voire une contradiction.

[81] Avis 15/2011 sur la définition du consentement du 13 juillet 2011, Groupe de travail « article 29 » sur la protection des données.

2.3.2.3.2. Le caractère potentiellement négociable de la durée de conservation

Le droit à l'effacement constitue à cet égard une véritable consécration du principe du consentement préalable aux traitements dont la portée est considérablement renforcée par le projet de règlement puisque le consentement peut être retiré. On se demande alors si la durée de conservation des données mais aussi les finalités des traitements n'ont pas vocation à devenir des éléments négociables avant que le consentement soit donné, faute pour le responsable d'imposer des conditions que la personne pourra aussitôt révoquer.

Il est donc tentant de considérer que le droit à l'effacement pourrait acquérir une certaine autonomie, véritable levier susceptible de bouleverser l'équilibre entre responsables de traitements et personnes concernées. Si l'insertion de l'article 17, paragraphe 1, dans les autres dispositions du projet de règlement plaide en faveur de cette lecture, ses autres paragraphes conduisent à relativiser ce jugement.

Pour mesurer l'impact de ces nouvelles dispositions, on peut essayer d'imaginer quelle serait la teneur d'une négociation en vue de la restitution des données. La menace de demande d'effacement avant l'expiration de la durée de conservation pourrait placer la personne en position de force pour obtenir la restitution et forcer le partage. Mais d'un autre côté, la menace de mise à exécution de l'effacement au terme de la durée de conservation est susceptible de redonner la main aux entreprises. Elles seront d'autant mieux armées que les données auront déjà été exploitées et n'auront plus d'intérêt par elles-mêmes.

Ceci montre à quel point il est important de savoir sur quoi portent en réalité la restitution ou l'effacement, sur la donnée brute ou sur la donnée déjà traitée et valorisée. Car la donnée personnelle est une information vivante dont la vie ne commence pas avec la collecte pour finir avec l'effacement. Et justement, quels que soient les liens qu'ils entretiennent, restitution et effacement posent le même problème de la définition des données concernées.

L'Agence Européenne chargée de la sécurité des réseaux et de l'information (ENISA) évoque la question en ces termes : « *A related question is how aggregated and derived forms of information (e.g. statistics) should be affected when some of the raw data from which statistics are derived are forgotten. Removing forgotten information from all aggregated or derived forms may present a significant technical challenge. On the other hand, not removing such information from aggregated forms is risky, because it may be possible to infer the forgotten raw information by correlating different aggregated forms* »[82].

[82] http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten.

S'agissant des données personnelles au sens large, il y aura vraisemblablement une tension entre un intérêt à effacer et un intérêt à récupérer.

Pour l'instant, le seul choix laissé aux individus est celui d'être ou ne pas être, d'accepter ou de supporter que leurs données soient traitées et de demander éventuellement l'effacement. Ainsi, l'article 17 maintient l'individu dans une certaine position de subalternité.

En conclusion de cette première partie, il apparaît que le droit positif a construit des mécanismes permettant l'accomplissement de l'oubli au profit des individus mais que ces derniers les connaissent mal ou les estiment extrêmement complexes. De façon très ciblée, le régime de protection des données personnelles témoigne d'une volonté affirmée du législateur d'offrir aux individus des instruments juridiques de contrôle de l'usage de leurs données personnelles par des tiers. Il n'a pas, dans ce cadre, été jugé nécessaire d'introduire explicitement un droit à l'oubli mais certaines prérogatives y conduisent inexorablement.

Pour autant, doit-on considérer que le dispositif est satisfaisant ? La mission Droit et justice soulignait l'absence de garanties quant à l'effacement des données. De notre point de vue, un droit à l'oubli ne saurait être réduit à un droit à l'effacement comme invitait à le penser l'article 17 de la proposition de règlement dans sa mouture initiale. On ne réécrit pas l'histoire. Le faire est même punissable pénalement. Ce qui perturbe l'oubli, qui l'empêche de s'accomplir, c'est avant tout la diffusion potentiellement permanente (et l'on songe ici surtout à la diffusion par Internet) ou la rediffusion (par exemple dans un article de presse ou une fiction du réelle) d'une information ou d'événements personnels. L'enquête sociologique en témoigne : la présence d'informations devenues obsolètes sur un réseau social est l'une des préoccupations des usagers.

L'effacement, le déréférencement, la fermeture d'un site, la limitation de la durée de conservation, mais également, et moins radicalement la non-diffusion des données ou le droit de masquage de certaines données, comme cela est prévu pour le Dossier Médical Personnel (DMP)[83], sont autant de modalités d'exécution possibles d'un droit à l'oubli. Mais toutes ne sont pas adaptées parce qu'elles n'ont pas été imaginées initialement comme une réponse à un droit à l'oubli.

En particulier, assimiler le droit à l'oubli à un droit à l'effacement des données comporte un risque et entame la légitimité d'un éventuel droit à l'oubli. Ainsi, l'effacement d'anciennes

[83] Le patient dispose d'un « droit de masquage » qui lui permet de rendre inaccessibles à certains professionnels de santé des données présentes dans son DMP. L'existence de documents masqués ne sera pas signalée. Voir CNIL, délibération n°2010-449 du 2 décembre 2010 portant autorisation des traitements de données personnelles mis en œuvre par les professionnels et établissements de santé nécessaires à la première phase de déploiement généralisé du dossier médical personnel.

publications licites ne se justifie pas toujours. Une simple restriction de la diffusion suffit parfois à faire cesser l'atteinte.

Assimiler le droit à l'oubli au droit à l'effacement procède également d'une erreur d'analyse car le droit à l'effacement ne saurait être considéré comme un droit subjectif[84]. Il assure, avec les autres modalités évoquées plus haut, le respect d'un droit subjectif, le droit à la protection des données personnelles. Ni plus, ni moins. Un exemple classique tiré du droit positif illustre pertinemment le propos : l'accouchement sous X, tel qu'il est règlementé en France, offre une sorte de droit à l'oubli à la mère. Or, l'accouchement sous X n'est validé que parce que l'administration conserve les données d'identification de la mère et n'a de sens que si ces données ne sont pas divulguées, notamment aux enfants. Dans cette hypothèse, l'effacement de l'information est exclu pour des raisons médicales. Le droit à l'oubli se traduit alors par une interdiction d'accéder aux données. Seul est coupé un lien vers l'information.

Sous cet angle, la rédaction de l'article 17 de la proposition de règlement telle qu'amendée nous semble plus pertinente que la précédente parce qu'elle ne donne pas l'illusion de créer un droit nouveau, qui substantiellement, n'est que très peu modifié.

A ce stade, au regard des résultats de l'enquête sociologique d'une part, et de l'analyse des dispositifs juridiques actuels, d'autre part, il convient donc de se demander si la consécration d'un droit à l'oubli autonome a encore du sens ? Pour répondre, il faut aller plus loin dans l'analyse du besoin exprimé par les personnes concernées. C'est que nous nous attacherons à vérifier en envisageant ce que pourraient être les contours d'un droit à l'oubli.

[84] En ce sens également J.M. Bruguière, « Le *droit à* l'oubli numérique, un droit à oublier » D.2014, p.299.

II. LES CONTOURS D'UN DROIT A L'OUBLI

La réflexion engagée quant aux contours d'un droit à l'oubli conduit à souligner d'emblée que le contentieux relatif au droit à l'oubli n'est pas cantonné aux données numériques. De notre point de vue, le numérique a amplifié le questionnement sur un éventuel droit à l'oubli mais ne saurait balayer les données non numériques du champ de la réflexion. Rien ne le justifie. L'article 17 de la proposition de règlement lui-même ne distingue pas entre ces deux types de données. Il est vrai que les cas les plus récurrents concerneront la diffusion numérique car c'est son ampleur qui est souvent source de préjudice. Il convient donc de procéder d'une approche large, seule capable d'identifier d'éventuels obstacles à un droit à l'oubli général et autonome. Afin de cerner les contours d'un droit à l'oubli, il convient de se demander quel serait l'objet d'un droit à l'oubli et à qui s'adresserait-il. Les contours du droit à l'oubli seront donc envisagés sous l'angle de son objet (1) et des acteurs concernés (2).

1. L'OBJET : QUE VEUT-ON PROTEGER ? LA NATURE DES INFORMATIONS CONCERNEES

L'examen des décisions judiciaires dans le cadre desquelles le demandeur invoque à l'appui de ses prétentions un droit à l'oubli démontre que le contentieux porte systématiquement sur des informations concernant la personne qui le revendique. Or, le droit positif comporte depuis de nombreuses années des qualifications et un statut juridiques pour les éléments qui concernent une personne. S'agissant de la qualification, nous l'avons évoqué en première partie, deux catégories pertinentes, et non exclusives l'une de l'autre, peuvent être mises en exergue. Il peut s'agir d'éléments de la vie privée ou bien encore de données à caractère personnel, catégorie large qui inclut des données très sensibles nécessitant une protection spécifique. Ces catégories ne sont pas complètement imperméables. Ainsi, une même information peut correspondre à une donnée à caractère personnel relevant de la vie privée mais ce n'est pas systématiquement le cas si bien que chaque qualification a son champ propre. En étudiant les liens entre le droit à l'oubli et le droit au respect de la vie privée, nous avons mis en avant les inconvénients qu'il y aurait à réduire le champ du droit à l'oubli aux éléments de la vie privée. Il n'y a pas lieu d'en faire de nouveau un objet d'étude spécifique, sauf à titre de comparaison. Nous nous concentrerons sur la seconde qualification juridique, celle de données à caractère personnelle.

Depuis la directive 95/46, la problématique de la protection des données a changé. Le développement d'Internet et l'avènement de la « Société de l'Information » en sont les facteurs essentiels. La protection des données doit permettre de lutter contre toutes atteintes liées à l'usage des données personnelles. Mais jusqu'où convient-il d'aller ? Doit-on traiter de la même façon des données *a priori* banales retraçant des événements du quotidien d'une personne diffusées par elle-même sur Facebook, Youtube ou Twitter, des données médicales et des informations à caractère pénal par exemple ?

En définitive, notre analyse sera guidée par l'objectif suivant : si à l'examen, il apparaissait qu'un droit à l'oubli permettrait de protéger d'autres informations que celles qui entrent dans la catégorie des données à caractère personnel, nous pourrions en déduire que cette qualification est insuffisante à protéger les personnes concernées par ces informations et considérer que la création d'un droit nouveau et autonome avec un objet propre se justifie.

Les données à caractère personnel, définition - Une donnée à caractère personnel n'est pas nécessairement un élément de la vie privé. Le nom patronymique par exemple, ne relève pas en lui-même, de la vie privée. La notion de données à caractère personnel renvoie immédiatement aux dispositifs spécifiques de protection de ces données.

Dans l'article 2 de la loi informatique et libertés de 1978, une donnée à caractère personnel est constituée par « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne ».

La proposition amendée de règlement sur la protection des données à caractère personnel se veut plus complète, les données à caractère personnel étant définies comme « toute information se rapportant à une personne physique identifiée ou identifiable (la "personne concernée"); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, par exemple à un nom, à un numéro d'identification, à des données de localisation, à un identifiant unique ou à un ou plusieurs éléments spécifiques, propres à l'identité physique, physiologique, génétique, psychique, économique, culturelle, sociale ou de genre de cette personne »[85].

[85] Article 4 §2.

Bien que ces définitions relativement ramassées donnent le sentiment d'une certaine uniformité, les données à caractère personnel présentent une très grande diversité et l'on peut considérer que peu d'informations sur la personne échappent à cette qualification ce qui la rend particulièrement intéressante face à la problématique du droit à l'oubli.

La caractéristique temporelle n'est pas absente de la protection des données à caractère personnel puisqu'on l'a vu, le législateur a accordé une attention toute particulière à la durée de conservation des données.

En outre, le législateur réserve aux données dites sensibles un régime plus protecteur que celui dont jouissent les autres données à caractère personnel. C'est le cas « des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci » (article 8 § I). En réalité, le législateur va plus loin et accorde une attention toute particulière à certaines données spécifiques. Il nous a semblé pertinent d'apporter un éclairage sur la manière dont le législateur français appréhende certaines données sensibles et tout spécialement, celles pour lesquelles un droit à l'oubli est[86] ou pourrait être revendiqué. C'est, notamment, le cas des données de santé (1.1), des données judiciaires (1.2) et des données relatives à l'état et à la situation personnelle et sociale de la personne (1.3).

1.1. Les données de santé

Mise en perspective, enjeux – A l'instar de nombreuses données, les données de santé sont confrontées à la numérisation de notre société. Destinées à circuler plus aisément, elles intéressent les opérateurs privés, comme publics, des entreprises qui développent des programmes pour téléphone aux chercheurs scientifiques.

L'avènement des puces RFID (*radio frequency identification*) ou des applications de téléphone pour la santé soulève des problématiques complexes, dans la mesure où les utilisateurs de ces nouvelles technologies n'ont pas toujours conscience de l'usage qui peut être fait de leurs données. Ce phénomène se conjugue avec les impératifs de maîtrise des dépenses de santé et d'amélioration de la santé publique et de la qualité de soins, qui réclament plus de

[86] Nous faisons là référence aux données pour lesquelles des demandes judiciaires de droit à l'oubli ont déjà été formulées et non à celles qui ressortent de l'étude sociologique puisque celle-ci n'a pas permis d'identifier de manière précise les données qui, selon les usagers, pourraient poser des difficultés.

transparence et un accès plus large aux données de santé[87]. La volonté de mettre en place une démocratie sanitaire, permettant de juguler les scandales sanitaires ou de mesurer la qualité de notre système de santé, abondent encore en faveur d'une ouverture plus importante des bases de données de santé[88].

Des concrétisations peuvent déjà être notées. Ainsi un dossier médical personnalisé et un dossier pharmaceutique ont vu le jour[89]. Des voix de plus en plus nombreuses sollicitent un accès plus libre à la base SNIIRAM (système national informationnel inter-régime d'assurance maladie) qui rassemble les informations anonymes relatives au remboursement des feuilles de soins par l'assurance maladie obligatoires, ainsi que les données hospitalières publiques et privées[90]. En 2009, l'Agence des systèmes d'information partagés de santé voit le jour, afin de favoriser le développement des partages d'informations de santé[91]. En juin 2013, la France a signé la charte du G8 pour l'ouverture des données publiques[92]. Une commission « Open data » a été créée sous l'égide du ministère des affaires sociales et de la santé.

Ces évolutions reposent avec acuité la question de la pertinence de la maîtrise des données personnelles, par le vecteur d'un droit à l'oubli, quelle que soit sa forme. Les données de santé sont intimement liées à l'être humain et à sa vie privée. Elles sont marquées du sceau de la confidentialité et du secret professionnel. Toute personne doit donc pouvoir accéder librement à ses données médicales, s'opposer à leur utilisation, voire demander leur effacement.

Définition– On cherchera en vain dans les textes nationaux une définition des données de santé[93]. Ainsi, en droit interne, l'article 8 de la loi de 1978 se contente-t-il de préciser qu'il « est interdit de collecter ou de traiter des données à caractère personnel (…) qui sont relatives

[87] Sur l'interférence entre les nouvelles technologies et le droit de la santé, voir notamment : N. Martial-Braz, « Données de santé », in *La proposition de règlement européen relatif aux données à caractère personnel : proposition du réseau Trans Europe experts*, sous la direction de Nathalie Martial-Braz, Société de Législation comparée, à paraître, p. 192 et s. ; L.Tilman, P. Frimat, « TIC et santé au travail : la protection des données de santé », JCP éd. S, nov. 2013, 1453 ; P. Desmarais, « Quel régime pour la m-Health », Comm. com. électr. 2013, n° 3, étude 5 ; D. Bourcier, P. de Filippi, « L'Open Data : l'universalité de principe et diversité des expériences », JCA éd. A, 2013, n° 38, 2260 ; B. Roussel, « Informatisation des dossiers médicaux en milieu hospitalier : intégrité et opposabilité des données numériques », Comm. com. électr. Juin 2009, étude 15.

[88] Au sujet de l'hôpital numérique, voir J.-F Forgeron et A. - L. Bénéat, « De la santé électronique à l'hôpital numérique », Gaz. Pal. 2009, n° 295, p. 5. ;

[89] S. Hocquet-Berg, « Le dossier médical personnel en questions… », RCA juin 2005, alerte 59. A propos de la commercialisation en ligne de médicaments, voir M. Griguer, « Pharmaciens et e-commerce, nouveau défi », Cah. de l'entrep., n° 1, janv. 2014, prat. 5.

[90] P.-L Bras, *Rapport sur la gouvernance et l'utilisation des données de santé*, remis à la Ministre des affaires sociales et de la santé en septembre 2013.

[91] J.Bossi, « Comment organiser aujourd'hui la protection des données de santé », RDSS 201, p. 208.

[92] Comp avec la Suisse : J. Jehl, « Suisse : vers un accès plus facile aux données publiques », JCP 2014, 317. Et plus largement en Europe : N. Ferraud-Ciandet, « L'union européenne et la télésanté », RTD eur. 2010, p. 537.

[93] On préfèrera ce terme à celui de données médicales, plus restrictif en ce que, par hypothèse, il se cantonne aux relations patients/médecins.

à la santé ». Le Chapitre X de ladite loi relatif aux traitements de données de santé à caractère personnel à des fins d'évaluation ou d'analyse des pratiques ou des activités de soins et de prévention, ne contient pas davantage de définition. Le Code de la santé publique adopte un silence similaire. L'article L. 1111-8 du CSP consent aux professionnels de santé ou à la personne concernée le droit de « déposer des données de santé à caractère personnel recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins auprès des personnes physiques ou morales agréées à cet effet », sans préciser la notion de données de santé.

Le droit international est plus prolixe. Une définition peut être trouvée dans un arrêt de la CJCE du 6 novembre 2003[94]. Une acception large est retenue. Sont qualifiés de données de santé tous les renseignements relatifs à l'état de la personne aussi bien physique que mental. Tel est d'ailleurs le sens conféré à la santé par l'OMS, qui l'entend comme un « état de bien-être physique, mental et social, et ne consiste pas seulement en une absence de maladie ou d'infirmité ». Adoptée en 1946, cette définition n'a pas été modifiée depuis[95]. Relèvent de cette qualification les maladies ou symptômes contractés, les traitements reçus, mais également la date du décès, les causes de celui-ci, les pratiques paramédicales, les soins esthétiques, les maladies virales, les grossesses et leur déroulement…

Le G29, dans un rapport adopté le 15 février 2007, prolonge cette définition. L'assertion données de santé « s'applique également aux données à caractère personnel lorsqu'elles présentent un lien clair et étroit avec la description de l'état de santé d'une personne : les données sur la consommation de médicaments, d'alcool ou de drogue et les données génétiques sont incontestablement des données à caractère personnel relatives à la santé (…) En outre, toutes autres données - par exemple données administratives (numéro de sécurité sociale, date d'admission à l'hôpital, etc.) – contenues dans les documents médicaux relatifs au traitement d'un patient doivent être considérées comme sensibles ». Le règlement européen n° 1338/2008 du Parlement européen et du Conseil du 16 décembre 2008[96] relatif aux statistiques communautaires de la santé publique et de la sécurité au travail, abonde en ce sens.

[94] Aff. C-101/01 : Rec. CJCE 2003, I, p. 12971.
[95] Préambule à la Constitution de l'Organisation mondiale de la Santé, tel qu'adopté par la Conférence internationale sur la Santé, New York, 19-22 juin 1946, signé le 22 juillet 1946 par les représentants de 61 Etats. 1946; (Actes officiels de l'Organisation mondiale de la santé, n° 2, p. 100) et entré en vigueur le 7 avril 1948.
[96] Voir les annexes I et II.

On se félicitera que l'article 4-12 de la proposition de règlement reprenne cette conception. Les données de santé y sont décrites comme « toute information relative à la santé mentale et physique d'une personne ou à la prestation de services de santé à la personne ». Le Parlement européen, dans sa résolution du 12 mars 2014, a ressenti le besoin de préciser que les données devaient être « à caractère personnel », laissant ainsi supposer qu'il existerait des données de santé qui n'obéiraient pas à cette caractéristique. On peut en douter.

Toutes les informations, qui gravitent autour de l'état physique et psychique d'une personne, quelles qu'elles soient, doivent recevoir la qualification de données de santé[97]. Ces données sensibles, en ce qu'elles touchent à l'intimité de l'être, doivent être appréhendées dans toutes leurs composantes et soumises à un régime protecteur commun.

Régime juridique –Le législateur accorde une attention particulière aux données de santé, qualifiées de données sensibles[98]. Ces dernières relèvent du champ de la loi Informatique et libertés, dont les principes ont été pour beaucoup repris dans le code de la santé publique. Par principe, tout traitement est prohibé. Les exceptions sont enserrées dans des conditions rigoureuses et doivent être entendues strictement[99].

Le principe : l'interdiction de tout traitement : Le principe, clairement énoncé à l'article 8 de loi de 1978, est l'interdiction et la collecte de toutes données relatives à la santé[100]. Ce principe est repris tant par la proposition de règlement européen à l'article 9-1 que par la résolution adoptée par le Parlement européen. La liste des exceptions peut cependant paraître longue et la formulation de certaines généreuse.

---

[97] Adde : CE, 19 juill. 2010, F. et C., JurisData n° 2010-012219 *:* constitue une donnée de santé à caractère personnel l'affectation d'un élève en classe d'insertion scolaire, dans la mesure où cette mention s'accompagne de précisions relatives notamment aux handicaps dont peut souffrir l'élève concerné.

[98] Article 9 du projet de règlement. Sur cette qualification de donnée sensible et le regret de son faible encadrement par la proposition de règlement, voir : N. Martial-Braz, J. Rochfeld, E. Gattone, » Quel avenir pour la protection des données à caractère personnel en Europe », D. 2013, p. 2788.

[99] F. Lesaulnier, « L'informatisation des données de santé et la législation Informatique et Libertés, in colloque Gouvernance et sécurité des systèmes d'information de santé », Marseille, juin 2001, http://www.ars.paca.sante.fr/fileadmin/PACA/Site_Ars_Paca/Nos_missions/Evenements/4_la_protection_des_donnees_de_sante_F_LESAULNIER_7_juin_2011_arspaca.pdf

[100] Pour une application : CE, 4 juin 2012, n° 334777, Section française de l'OIP : JurisData n° 2012-012211 ; JCP A 2012, act. 415, note C.-A. Dubreuil ; Comm. com. électr. 2012, comm. 116, note A. Lepage : au sujet du cahier électronique de liaison mis en place par le ministère de la Justice au sein des établissements pénitentiaires sans qu'aucune formalité n'ait été faite auprès de la CNIL, le conseil d'Etat a fait droit à la demande de suppression de ce fichier. En application de l'article 26 de la loi Informatique et libertés, ce cahier aurait dû être autorisé par décret en Conseil d'Etat, après avis de la CNIL, dès lors qu'il contenait des informations relatives à la santé et à la pratique religieuse des détenus.

Exceptions - D'abord, la personne concernée peut donner son consentement exprès[101] à cette utilisation[102]. L'article 8-1° de la loi de 1978 a été dupliqué dans des textes spéciaux, afférents par exemple au dossier médical personnalisé ou au dossier pharmaceutique[103]. La proposition de règlement livre une définition opportune du consentement[104] à l'article 4-8. La proposition du Parlement précise en outre pertinemment que le consentement porte tant sur le principe du traitement, que sur la finalité de celui-ci, qui par hypothèse aura dû être portée à la connaissance de l'intéressé[105]. Le consentement doit être clair et sans équivoque, même si un écrit n'est pas requis à titre de validité[106].

Ensuite, le législateur s'accommode de l'absence de consentement lorsque le traitement obéit à des finalités qu'il énumère.

Ainsi entre professionnels de soins, la collecte des données de santé est permise dès lors qu'elles accompagnent des actes de prévention, de diagnostic, de soins et de traitements[107]. Le secret médical auxquels sont tenus ces praticiens préserve le patient de toute diffusion inopinée. De même, les traitements nécessaires à la recherche dans le domaine de la santé sont conditionnés à des modalités précises énoncées par le chapitre IX de la loi informatique et libertés. Entrent dans le cadre de cette disposition notamment les recherches biomédicales. En outre, si les données font l'objet d'un procédé d'anonymisation[108] préalablement reconnu conforme à la loi par la CNIL, celle-ci peut autoriser, compte tenu de leur finalité, certaines catégories de traitements selon les modalités prévues à l'article 25 de la loi de 1978. Le consentement n'est pas non plus exigé si le traitement est nécessaire à la sauvegarde de la vie humaine et que la personne concernée est dans l'incapacité de donner son consentement. Enfin, les traitements justifiés par l'intérêt public sont également envisageables. Participent de ce tempérament les traitements organisés par l'assurance maladie[109] ou encore le dossier médical personnel.

---

[101] Il convient de noter qu'en certains cas le consentement est impuissant à lever l'interdiction du traitement de données. Voir par exemple à propos du dossier médical personnel, article L. 1111-18 alinéa 2 du CSP : « L'accès au dossier médical personnel est notamment interdit lors de la conclusion d'un contrat relatif à une protection complémentaire en matière de couverture des frais de santé et à l'occasion de la conclusion de tout autre contrat exigeant l'évaluation de l'état de santé d'une des parties. L'accès à ce dossier ne peut également être exigé ni préalablement à la conclusion d'un contrat, ni à aucun moment ou à aucune occasion de son application ». De même ce dossier n'est pas accessible dans le cadre de la médecine du travail.

[102] Pour une application : C. Le Goffic, « Consentement et confidentialité à l'épreuve de la télémédecine », RDSS 2011, p. 987.

[103] Articles L. 1111-14 du Code de la santé publique et suivants ; articles L. 161-36-1 et suivants du même code ;_ Voir également l'article L. 1111-8 alinéa 1 du CSP.

[104] Sur la forme du consentement, voir articles 7 et 8 du projet de règlement.

[105] Amendement 103 à l'article 9.

[106] Adde : Cass. crim., 24 févr. 2009, n° 08-84.436. : JurisData n° 2009-047348.

[107] La norme simplifiée n° 50 adoptée par la CNIL le 22 novembre 2005 définit les caractéristiques des traitements litigieux.

[108] C'est sous couvert de cet anonymat qu'ont été autorisés les traitements par certaines sociétés privées d'assurances maladie complémentaire pour pouvoir avoir accès à des données issues des feuilles de soins électroniques, afin d'adapter leurs garanties. Sur ce point, voir J. Bossi, art. préc.

[109] Article L. 161-29 CSS.

La proposition de règlement et la résolution du Parlement retranscrivent peu ou prou ces tempéraments. L'article 9 § II reprend par exemple le consentement au traitement, la sauvegarde des intérêts vitaux de la personne, ou les finalités liées à la santé. Ces dernières sont précisées par l'article 81 du texte.

Le traitement des données en question est légitimé lorsqu'il est opéré par des professionnels soumis au secret médical aux fins de « médecine préventive, diagnostics médicaux, de l'administration de soins ou de traitement ou encore de la gestion de service de santé ».

Il en est de même lorsqu'il est justifié par « des motifs d'intérêt général dans le domaine de la santé publique, tel que la protection contre les menaces transfrontières graves pour la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité, entre autres pour les médicaments ou les équipements médicaux ». Cette liste ne se veut pas exhaustive et on peut regretter la généralité de ce motif qui laisse place à une interprétation incertaine, même si la Commission est autorisée à adopter des actes délégués pour contenir cette notion. Le point c) de cet article autorise encore le traitement de données de santé « pour d'autres motifs d'intérêt général dans des domaines tels que la protection sociale, particulièrement afin d'assurer la qualité et la rentabilité en ce qui concerne les procédures utilisées pour régler les demandes de prestations et de services dans le régime d'assurance-maladie ».

La référence aux motifs d'intérêt général et d'intérêt public appelle une certaine prudence, tant le contenu de ces notions est évasif et évolutif. Il peut être interprété comme une concession faite à certains acteurs privés économiques (mutuelles, assurances) désireux d'accéder à des sources riches de potentialités, sans avoir besoin de solliciter le consentement de l'intéressé, ni même de dispenser une information.

Enfin, les données relatives à la santé peuvent encore être traitées à des fins de recherche historique, statistiques ou scientifique, « tels que les registres de patients établis pour améliorer les diagnostics, distinguer entre des types de maladies similaires et préparer des études en vue de thérapies », sous réserve de leur anonymisation prévue à l'article 83 de la proposition de règlement. La résolution du Parlement semble revenir sur cette exception. Il n'admet la collecte de données dans cette hypothèse qu'avec le consentement de l'intéressé et toujours sous couvert d'anonymisation, là où la proposition de règlement ne réclamait le consentement que pour la divulgation des informations.

Droit de retrait, d'opposition et de rectification, durée de conservation (renvoi) – Les patients dont les données sont collectées bénéficient naturellement des droits instituées par la loi de 1978 comme le droit de retrait, d'opposition, de rectification, ou encore à une durée limitée de conservation[110]. Ceux-ci peuvent connaître certains aménagements par rapport au « droit commun » afin d'accroître la protection de ces données sensibles. C'est ainsi qu'un patient a en principe un droit d'accès libre et illimité à son dossier médical personnel et qu'il peut le supprimer à tout moment. Il doit pouvoir également limiter les professionnels pouvant le consulter ou encore dissimuler certaines informations[111]. De même, le droit d'opposition à un traitement des données de santé à des fins de recherches médicales[112] n'est conditionné par aucun motif légitime, contrairement au droit d'opposition de 38 de la loi informatique et libertés. Concernant le droit d'accès, l'article 43 de la loi de 1978 dispose que les données de santé « peuvent être communiquées à la personne concernée, selon son choix, directement ou par l'intermédiaire d'un médecin qu'elle désigne à cet effet dans le respect des dispositions de l'article L.1111-7 du Code de la santé publique ».

La protection de ces données est encore assurée par un contrôle accru de la mise en œuvre des traitements et par l'anonymisation des données en certains cas.

Contrôle administratif *a priori*[113]- Un contrôle administratif *a priori* est censé suppléer l'absence de recueil de consentement au traitement des données de santé. Ainsi aux termes des articles 22 et suivants de la loi de 1978, le traitement doit faire l'objet d'une déclaration préalable auprès de la CNIL par le responsable de traitement. Les traitements visés à l'article 25 doivent en outre être autorisés, soit par la CNIL, soit par un arrêté. Parmi ceux-ci figurent notamment le traitement de données anonymes ou celui motivé par l'intérêt public. La demande doit comporter plusieurs mentions obligatoires et notamment la finalité du traitement et la durée de conservation, le service ou la fonction de la personne auprès desquels s'exerce le droit d'accès de l'article 39.

Un dispositif particulier, décrit aux articles 53 et suivants de la loi informatique et libertés, a été institué pour le traitement de données ayant pour fin la recherche de la santé dans le domaine de la santé. En substance, le comité consultatif sur le traitement de l'information en

[110] Voir *supra*.
[111] Articles L. 1111-14 et suivants du CSP.
[112] Article 56 de la loi informatique et liberté.
[113] Sur le contrôle *a posteriori*, voir *infra*.

matière de recherche dans le domaine de la santé (CCTIRS) donne un avis sur la recherche et sur le traitement des données. Cet avis est transmis à la CNIL qui fait droit ou non à la demande.

Une même autorisation pour le traitement des données de santé est prévue par l'article 33 du projet de règlement. Au préalable, une analyse d'impact devra être réalisée par le responsable pour les études de grande échelle.

L'anonymisation – Une autre garantie offerte aux personnes dont les données sont exploitées réside dans leur anonymisation, permettant ainsi à ces dernières d'être oubliée dans la masse. Elles deviennent un nombre parmi d'autres nombres, en principe non identifiables. Cette modalité d'oubli et de préservation des droits des patients est institutionnalisée à l'article 8-III de la loi de 1978[114]. Néanmoins, elle présente des faiblesses ainsi que l'a constaté l'IGAS dans son rapport remis à la ministre de la santé en 2013[115]. La mise en place longue et complexe du dossier médical personnel illustre les limites inhérentes à l'anonymisation. L'accès au DMP suppose en effet que le patient puisse être identifié de manière certaine, tout en conservant son anonymat. Pour l'heure, l'expérience se heurte à la mise en place de cet identifiant national de santé pour chaque patient fiable[116].

Le dispositif offre incontestablement des garanties aux patients dont les données médicales sont collectées. Il n'en reste pas moins que le passé médical laisse des traces qui dans notre société, demeurent pénalisantes dans certaines situations. Il suffit d'évoquer la situation des personnes qui ont été victimes de cancer lorsqu'elles souhaitent obtenir un crédit. La revendication des anciens malades en rémission porte sur la mise en place d'un droit à l'oubli social, notamment bancaire, à défaut duquel ils se voient appliquer des taux d'assurances très élevés[117]. L'institut national du cancer plaide pour un droit à l'oubli *stricto sensu* qui permettrait aux anciens malades, dans des délais adaptés à chaque pathologie, de ne plus faire mention de leur cancer passé sur le questionnaire de santé, préalable à tout emprunt. De leur côté, les représentants des assureurs exigent le maintien de cette déclaration préalable et s'engagent à adapter le calcul du risque aux nouveaux chiffres de mortalité et de récidive fournis par les autorités. Entre ces intérêts divergents, l'arbitrage demeure complexe et la consécration d'un droit à l'oubli difficile.

---

[114] Voir également les articles 55 et 63 de la loi informatique et libertés.
[115] P.-L Bras, rapport préc., p. 26 et s.
[116] N. Martial-Braz, *op. cit*., p. 201 ; J. Bossi, art. préc.. Voir également les développements consacrés à l'effectivité technique du droit à l'oubli.
[117] http://www.lefigaro.fr/vox/societe/2015/02/04/31003-20150204ARTFIG00156-journee-mondiale-du-cancer-pour-un-droit-a-l-oubli.php

1.2. Les données judiciaires

Parmi les données judiciaires, certaines sont plus sensibles que d'autres – les données pénales par exemple – mais toutes méritent protection et suscitent une question d'une acuité particulière au regard du droit à l'oubli. L'article 9 §2, j) de la proposition de règlement amendée prévoit d'ailleurs de manière encore plus large que le cadre judiciaire dans lequel nous inscrivons notre réflexion que « le traitement des données relatives aux sanctions administratives, aux jugements, aux infractions pénales, aux condamnations ou aux mesures de sûreté connexes est effectué soit sous le contrôle de l'autorité publique, ou lorsque le traitement est nécessaire au respect d'une obligation légale ou réglementaire à laquelle le responsable du traitement est soumis, ou à l'exécution d'une mission effectuée pour des motifs importants d'intérêt général, dans la mesure où ce traitement est autorisé par le droit de l'Union ou par la législation d'un État membre prévoyant des garanties adéquates pour les droits fondamentaux et les intérêts de la personne concernée. Tout registre des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique ». Les données pénales présentent la spécificité d'être répertoriées dans un registre dédié, le casier judiciaire dont l'existence et le régime juridique démontrent que le droit à l'oubli est un impératif du système judiciaire dont il constitue une des composantes sociales puisqu'il agit comme un régulateur de la mémoire sociale. L'ensemble des données judiciaire peut néanmoins se retrouver dans des banques de données

1.2.1. Les données pénales et le casier judiciaire[118]

Remplaçant un système d'information obsolète, le casier judiciaire est né d'une circulaire du garde des Sceaux du 6 novembre 1850. Mis en place afin de préserver la mémoire *judiciaire* du passé pénal des citoyens, le casier judiciaire (actuellement dénommé casier judiciaire national informatisé) connut rapidement un dévoiement en fait : accessible à tous, il devint un outil de mémoire *sociale* et, corrélativement, « l'instrument d'une peine accessoire universelle »[119], une (potentielle) atteinte durable à la réputation doublant de fait toute

[118] Ce texte est consacré au casier judiciaire des seules personnes physiques. L'institution d'un principe de responsabilité pénale des personnes morales lors de la refonte du Code pénal en 1992 a conduit à instituer un casier judiciaire des personnes morales sur le même modèle. Quelques différences qui ne tiennent pas à de simples ajustements techniques mais à un choix politique seront cependant signalées en contrepoint dans les lignes qui suivent. Elles illustrent une conception propre à cet objet : soucieux de préserver la compétitivité des entreprises françaises, le législateur a défini un régime restrictif pour le casier des personnes morales.

[119] J.-H. Robert, *Droit pénal général*, PUF, coll. Thémis, 6e éd., 2005, p. 543.

condamnation pénale et entre, de ce fait, dans le cadre du questionnement sur l'existence d'un droit à l'oubli.

La difficulté vient de ce que ses fonctions ne sont pas nécessairement convergentes.

De manière sommaire, la fonction judiciaire conduit plutôt à organiser une mémoire aussi complète que possible : l'application de la loi pénale requiert que le juge dispose d'une information de qualité sur le passé de l'agent qui comparaît devant lui. Le régime de la récidive, l'applicabilité de certaines dispositions en matière de peine (applicabilité du sursis par exemple), le simple exercice du pouvoir général d'arbitrage de la peine dont dispose le juge de jugement dans la limite du maximum légal institué par la loi sont quelques exemples des enjeux qui s'attachent à la mémoire judiciaire du passé de l'agent. Dans cette perspective, une problématique nouvelle tient à la mise en place d'un casier judiciaire européen, consistant moins en un casier supranational sur le modèle des casiers nationaux qu'en une interconnexion des casiers étatiques.

Inversement, la fonction extra-judiciaire, lourde de dangers en termes de droits des personnes et de libertés publiques, impose un contingentement d'une information éminemment sensible. Le souci du législateur contemporain du reclassement des délinquants a d'ailleurs conduit à un regain d'attention sur ce point.

C'est en contemplation de ces exigences parfois contradictoires que la loi organise le casier judiciaire. Deux outils sont mobilisés par le droit : le contenu et l'accessibilité du casier judiciaire.

1.2.1.1. Contenu

Le contenu du casier judiciaire est fonction des flux qui le façonnent : l'entrée d'une information dans le système peut être suivie de sa sortie. La ligne qui résume sommairement la politique législative en la matière est simple : autorisée par un flux d'entrée puissant, la relative complétude du casier judiciaire est assurée par une stricte définition du flux de sortie.

Les informations entrant dans le système sont de deux ordres : aux informations principales lesquelles tiennent à la mise en œuvre de la répression s'ajoutent des informations correctives.

- Informations premières : les informations à inscrire au casier judiciaire sont très largement définies par la loi[120]. En d'autres termes, il n'est guère d'oubli *ab initio.* La plupart des condamnations pénales doivent y être portées. Font exception, par disposition de la loi,

[120] C. proc. pén., art. 768.

certaines condamnations pour les contraventions des quatre premières classes (les moins graves). Fait également exception, si le juge en décide ainsi, la décision de condamnation assortie d'une dispense de peine[121]. Ce cas particulier est révélateur d'une tendance contemporaine : organiser l'oubli afin de favoriser ou, plus exactement ici, cristalliser le reclassement de l'agent.

Enfin, au-delà même du champ pénal, des données sont collectées, qui intéressent l'exercice des droits politiques et civils, notamment de famille – ainsi des jugements prononçant la déchéance de l'autorité parentale ou de certaines décisions frappant les personnes physiques dans le cadre des procédures collectives.

- Informations correctives : afin de restituer exactement la répression exercée contre l'agent, le casier judiciaire intègre la mention d'évènements venant corriger sa mise en œuvre. Ainsi d'une grâce ou d'une libération conditionnelle[122]. Il en va de même, en principe, d'une réhabilitation, qu'elle intervienne de plein droit ou sur décision de justice. La chose mérite d'être relevée : l'incidence de la réhabilitation sur le contenu du casier judiciaire a varié, le législateur ayant un temps opté pour une mesure plus radicale que celle qui vient d'être exposée, savoir le retrait pur et simple de la condamnation[123].

Sortie – Les informations entrées dans le casier judiciaire n'y restent certes pas éternellement. L'oubli d'une information enregistrée a sa place dans le fonctionnement du casier judiciaire. Le législateur contemporain a même semblé vouloir lui faire une place accrue[124].

[121] C. proc. pén., art. 768 et C. pén., art. 132-59, al. 2. Si, en règle générale, le prononcé de la culpabilité appelle celui d'une ou plusieurs peines en répression, la loi autorise le juge, en matière correctionnelle et contraventionnelle, à dispenser le condamné de peine. Trois conditions cumulatives sont requises : il faut que le reclassement du coupable soit acquis, le dommage réparé et que le trouble né de l'infraction ait cessé (C. pén., art. 132-59, al. 1er).

[122] C. proc. pén., art. 769.

[123] Aux termes de la loi du 5 mars 2007, le retrait de la condamnation peut suivre une réhabilitation si celui-ci en décide ainsi. Il ne s'agit donc plus d'un effacement de plein droit mais d'un effacement sur décision expresse. D'aucuns y voient une marque de la supériorité de la mémoire sur l'oubli dans la politique législative des années 2000.

[124] Evoquant « un droit à l'oubli » reconnu aux délinquants par le législateur, v. not. Fr. Desportes et Fr. Le Gunehec, *Droit pénal général*, Economica, 16e éd., 2009, n° 1144, p. 1085). Si l'idée générale n'est pas fausse, la qualification ne peut être retenue : on ne voit pas de droit subjectif sous ce mécanisme. De plus, il faudrait démontrer que la faveur pour l'agent est le fondement de tous les mécanismes envisagés. Au moins à titre d'hypothèse, on peut penser que certaines mesures d'effacement sont moins motivées par la protection des personnes que par la gestion technique du système. On songe ici à l'effacement pour cause de mort (C. proc. pén., art. R 70, qui, à défaut d'avis du décès, prévoit l'effacement « quand le titulaire aurait atteint l'âge de cent ans »).

Certaines données sont effacées de plein droit. C'est le cas s'il y a amnistie[125] ou après un certain temps. Les délais et éventuelles conditions de mise en œuvre varient selon la condamnation envisagée. Par exemple, si une nouvelle condamnation à une peine criminelle ou correctionnelle n'est pas intervenue dans l'intervalle, les condamnations les plus graves prononcées contre les majeurs sont retirées du casier à l'expiration d'un délai de quarante ans à compter de leur prononcé[126]. A titre de comparaison, les condamnations pour contravention sont, en principe, retirées trois ans après la date à laquelle elles sont devenues définitives. Il est intéressant de noter qu'un délai de trois ans à compter du prononcé est également retenu pour les condamnations contre les mineurs – sous réserve de l'absence de facteurs d'exclusion, parmi lesquels une condamnation à une peine criminelle ou correctionnelle. La protection du mineur a en effet soulevé des discussions particulières dans le cadre de la proposition de règlement sur la protection des données à caractère personnel[127] et ces dispositions particulières témoignent du souci du législateur d'assurer aux mineurs une protection accrue de leurs données.

Enfin, le juge peut, dans de rares cas, décider du retrait d'une information portée au casier. L'hypothèse principale est prévue par l'article 770 du Code de procédure pénale lequel organise une possibilité d'effacement judiciaire s'agissant des mineurs (même devenus majeurs) et, dans des conditions plus strictes, des jeunes majeurs (âgés de 18 à 21 ans à la date des faits).

Fidèle à l'idée d'une spécificité de la délinquance des mineurs et, dans une moindre mesure, des jeunes majeurs, de par leur immaturité, la loi prévoit ici un dispositif de faveur en donnant au juge la possibilité d'ordonner le retrait de condamnations prononcées contre eux.

1.2.1.2. Accessibilité

L'accessibilité tient essentiellement à deux mécanismes[128]. Classiquement, elle consiste en la possibilité de se faire délivrer un extrait du casier. A la fin du XXe siècle, un droit de

[125] L'amnistie, supposant une loi, efface rétroactivement la qualification pénale du fait. Il faut noter cependant que la pratique législative en matière d'amnistie a progressivement changé au tournant du XXe et du XXIe siècle. En termes politiques, la forme commune de l'amnistie était devenue, dans un pays pacifié depuis la fin des guerres coloniales, l'amnistie dite présidentielle, forme contemporaine de don de joyeux avènement. De plus en contestée, cette vieille pratique a régressé avant de cesser complètement : si l'élection présidentielle de 2002 avait été suivie d'une loi d'amnistie plus restrictive, celles de 2007 et 2012 n'ont pas donné lieu à une telle mesure. Par où le droit pénal contemporain marque également une volonté de mémoire.

[126] Une exception est notamment prévue pour les condamnations prononcées pour des « faits imprescriptibles (sic) », autrement dit des faits tombant sous une qualification pénale pour laquelle la loi écarte la prescription de l'action publique (ainsi des crimes contre l'humanité).

[127] Article 17 §1 de la proposition de 2012 l'article 17 §1 évoquait le cas des personnes ayant rendu leurs données disponibles lorsqu'elles étaient enfants.

[128] Aux deux mécanismes mentionnés au texte, il faut ajouter un troisième : il est des copies délivrées d'office pour communiquer à certains organismes publics des éléments nécessaires à l'exercice d'une mission particulière. C'est ainsi que, chargé de l'établissement des listes électorales, l'INSEE est tenu au courant des condamnations qui emportent déchéance du droit de vote.

consultation générale, réservé à la personne « titulaire » du casier, est venu compléter le dispositif.

La délivrance d'extraits de casier judiciaire – L'accès à l'information contenue dans le casier judiciaire se fait essentiellement par l'envoi de copies d'un des bulletins composant le casier. Imaginée à la fin du XIXe siècle, l'organisation en bulletins a une fonction simple : maîtriser l'accès à l'information en faisant varier les cercles de diffusion potentielle.

Le casier judiciaire est organisé en trois bulletins, désignés par un numéro : 1, 2, 3. Leur régime varie, et quant à leur contenu, et quant à leur accessibilité. Le système est ainsi conçu qu'il existe une relation inversement proportionnelle entre contenu et accessibilité. Du bulletin n° 1 au bulletin n° 3, l'information s'épure, par le jeu de sélections successives. Corrélativement, du bulletin n° 1 au bulletin n° 3, le cercle des personnes pouvant prétendre à l'information s'élargit.

Le bulletin n° 1 est destiné essentiellement aux autorités judiciaires[129] dans l'exercice de leur pouvoir de répression. Puisqu'il contient l'ensemble des informations inscrites au casier judiciaire de la personne à un instant *t*, il leur assure une information relativement complète sur le passé pénal de l'agent[130]. Le bulletin n° 1 est donc l'instrument privilégié de la fonction de mémoire judiciaire du casier : une mémoire riche et longue aux (seules) fins d'application de la loi pénale.

Le bulletin n° 2 est moins riche en même temps que plus largement accessible. Son contenu est moindre que le bulletin n° 1, la loi imposant une sélection parmi les informations inscrites au casier judiciaire[131]. Les critères de sélection sont principalement de deux ordres. Il est tenu compte de la nature de la décision. Par exemple, les condamnations pour contravention de police ne figurent pas au bulletin n° 2. Il est également tenu compte de l'agent : les décisions prises contre les mineurs sont omises du bulletin n° 2. A ces exclusions légales qui opèrent de plein droit, peuvent s'ajouter des omissions décidées par le juge. Sauf exceptions, la loi attribue au juge la faculté d'exclure*, ab initio* ou *a posteriori*, la mention de la condamnation au bulletin n° 2. La diffusion de celui-ci est sensiblement plus large que celle du bulletin n° 1 : il est

[129] Une loi du 17 mai 2011, ajoutant un alinéa 3 à l'article 774 du Code de procédure pénale, autorise désormais la communication du bulletin n° 1 aux greffes des autorités pénitentiaires à des fins d'exécution des peines.
[130] La force probante du bulletin n° 1 est toutefois limitée. Parce qu'il ne s'agit que d'une copie de copie et qu'il est un risque d'erreur lié notamment à une possible usurpation d'identité, la jurisprudence décide que le bulletin n° 1 ne fait foi que dans la mesure où il n'est pas réfuté par l'agent. En d'autres termes, les éléments contenus par le bulletin n° 1 devront être autrement établis si l'agent conteste celui-ci.
[131] C. proc. pén., art. 775.

accessible à un certain nombre de personnes[132], essentiellement des autorités publiques à des fins d'administration – ainsi pour l'octroi d'un emploi public ou d'un marché public[133]. Le bulletin n° 2 participe donc de la fonction de mémoire sociale du casier judiciaire. Quoique la liste des destinataires s'élargisse, il la corrèle cependant à la préservation de l'intérêt public.

Contrairement aux précédents, le bulletin n° 3 est un reflet très déformé du casier judiciaire. L'information qu'il offre est largement expurgée par rapport au contenu réel qui peut être celui du casier[134]. D'une part, seules les condamnations les plus graves peuvent y figurer – ainsi des condamnations à une peine privative de liberté d'une durée supérieure à deux ans sans bénéfice du sursis. D'autre part, la loi octroie au juge pénal de larges pouvoirs pour moduler le contenu du bulletin n° 3. Contrairement à ce qui est prévu pour le bulletin n° 2, le pouvoir judiciaire de modulation peut cependant s'exercer dans les deux sens : non-inscription ou retrait d'une information prévue par la loi d'une part, inscription d'une information non prévue par la loi d'autre part. Cette hyper-sélectivité du bulletin n° 3 est liée à son accès ouvert : le titulaire du casier peut obtenir copie du bulletin n° 3. En pratique, l'usage s'en était répandu dès le XIXe siècle, la demande de la personne est motivée par la requête que lui adresse un tiers : c'est pour satisfaire la curiosité d'un possible employeur, logeur…, que la personne demande copie de son bulletin n° 3[135]. En d'autres termes, l'information offerte par le bulletin n° 3 est quasi-publique en fait. Plus exactement, la loi ne pose aucune règle qui contrarie l'avidité du corps social. Pire, le législateur a intégré cette fonction sociale diffuse du casier judiciaire en donnant au juge un pouvoir de modulation de son contenu : pourquoi moduler sinon pour préserver l'agent du retentissement social de sa condamnation ou, à l'inverse, pour lui faire subir celui-ci ? Le bulletin n° 3 fait du casier judiciaire un instrument de répression indirecte et extra-juridique : il permet l'exercice d'un contrôle social fondé sur le passé pénal de la personne. La contre-épreuve est fournie par le régime du casier judiciaire des personnes morales : il ne compte que les bulletins 1 et 2 afin de préserver les intéressés des risques socio-économiques que porte l'existence du bulletin n° 3. C'est naturellement dans ce cadre que se pose avec acuité la question du droit à l'oubli.

---

[132] C. proc. pén., art. 776 et art. R 79. La liste va même s'allongeant, le législateur ayant abandonné au pouvoir réglementaire le pouvoir de compléter les dispositions légales sur ce point. Cette tendance observée pour les personnes physiques contraste avec la prudence du législateur s'agissant des personnes morales (C. proc. pén., art. 776-1). Sur ce point comme sur d'autres, la loi se fait restrictive par crainte que la réputation des entreprises françaises, élément de leur compétitivité, ne soit mise en cause, notamment sur le plan international.

[133] Par suite, on peut considérer que « ce bulletin n° 2 fonctionne comme une peine accessoire d'interdiction professionnelle. » (J.-H. Robert, *op. cit.*, p. 547).

[134] C. proc. pén., art. 777.

[135] Conscient des dérives auxquelles le système initial donnait lieu, une circulaire du garde des Sceaux avait, en 1876, mit un terme à l'accès général au casier judiciaire pour en exclure les simples tiers. La pratique n'avait pas tardé à déjouer cette garantie : lesdits tiers, privés d'un accès direct au casier d'autrui, exigeaient, lorsqu'ils en avaient les moyens, qu'il leur communique l'information qu'il pouvait seul obtenir directement… C'est pour contenir cet usage délétère que la loi de 1899 a imaginé la division en bulletins dont le dernier, seul accessible à l'intéressé, est expurgé.

Le droit de consultation du titulaire – En application du droit commun relatif à l'accès aux données publiques, spécialement celles qui sont informatisées, la loi attribue à la personne le droit de consulter son casier judiciaire[136].

La personne a ainsi un accès à l'information dans son ensemble : c'est le casier en son entier qui lui est alors accessible, non le seul bulletin n° 3.

Cependant, fidèle à la logique du rapport inversement proportionnel entre contenu et accessibilité, la loi ne permet qu'une consultation : l'intéressé ne peut obtenir une copie à ce titre. Mieux : instruit par l'histoire des risques de dérives, le législateur a institué une incrimination pénale afin de garantir la limitation du droit de consultation. Le tiers qui obtiendrait de l'intéressé les éléments issus de la consultation de son casier est passible d'une amende pénale.

Outre le casier judiciaire, il existe des systèmes de traitement des données personnelles en matière pénale : STIC, JUDEX et TPJ.

Le « **système de traitement des infractions constatées (STIC) »** est un fichier national appelé à enregistrer les informations recueillies par les fonctionnaires de la police nationale dans le cadre de leurs missions de police judiciaire relatives aux crimes, aux délits et à six catégories de contraventions de la 5ème classe.

Il a pour objet de permettre la rationalisation du recueil et de l'exploitation des informations de police judiciaire aux fins de recherches criminelles, de production de statistiques et de gestion des archives. Il pourra aussi dans certaines conditions, être consulté à des fins de police administrative. Ainsi, l'interrogation du STIC peut s'effectuer, pour une recherche simple, à partir d'un ou deux critères, tels que le nom et la date de naissance d'une personne : il s'agira alors de vérifier les antécédents d'une personne déterminée[137].

Le « **système d'information judiciaire » JUDEX**, comme le "système de traitement des infractions constatées" (STIC) mis en œuvre par la police nationale, constitue un traitement de données à caractère personnel dont les principes de fonctionnement sont fixés par la loi du 18 mars 2003 s'agissant en particulier des finalités de ces fichiers, de leurs modalités

[136] C. proc. pén., art. 777-2.

[137] Voir tout de même la décision de la CEDH du 18 septembre 2014 qui condamne le fonctionnement du STIC en ce qu'il porte atteinte à la vie privée, A. Debet, « Une condamnation attendue : le fonctionnement du STIC jugé contraire au droit au respect de la vie privée ! », Comm. Comm. Electr. 2014, comm. 97.

d'alimentation et de mise à jour, des catégories de personnes susceptibles d'être inscrites dans ces fichiers et des destinataires des informations.

Il a pour objet de faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs.

Le « **traitement de procédures judiciaires** » (TPJ), initialement développé sous l'acronyme ARIANE (Application de Rapprochement, d'Identification et d'ANalyse pour les Enquêteurs), sera un fichier d'antécédents au sens des articles 230-6 et suivants du Code de procédure pénale, dispositions introduites par la loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.

Il a vocation à devenir les fichiers d'antécédents communs à la police et à la gendarmerie nationale et donc de remplacer le STIC et le système JUDEX mais compte de dysfonctionnements importants sa création a été reportée à 2015.

La CNIL avait apporté un certain nombre de garanties sur le STIC et le système JUDEX dans plusieurs avis[138]. Une des principales craintes exprimées par les interlocuteurs auditionnés sur la mise en œuvre de ces systèmes de traitement est leur utilisation tel un « casier judiciaire bis » alors qu'il n'offre pas les garanties prévues pour le fonctionnement du casier judiciaire national. Ainsi, la Commission s'est engagée à ce que la finalité exclusivement policière des fichiers soit rigoureusement respectée.

La règlementation applicable au casier judiciaire permet d'éviter les dérives les plus significatives car le risque est faible que ces données se retrouvent en libre accès sur Internet. Le cadre juridique est suffisamment strict pour que l'on n'ait pas à en faire une préoccupation majeure de la problématique actuelle du droit à l'oubli précisément, parce que le contrôle de la mémoire sociale et corrélativement, le droit à l'oubli, ont été intégrés dès le départ. Le passé judiciaire, même numérisé, est de ce fait sous contrôle. Il en va différemment lorsque les données judiciaires sont stockées dans des banques de données.

[138] Notamment, Délibération n°00-064 du 19 décembre 2000 portant création du "Système de Traitement des Infractions Constatées TIC)" et application du troisième alinéa de l'article 31 de la loi du 6 janvier 1978. Délibération n°2005-188 du 8 septembre 2005 portant sur l'application de l'article 26 (II) de la loi du 6 janvier 1978 modifiée et portant création du système d'information judiciaire « JUDEX ». Ce ne sont pas les plus récents mais sans doute les plus instructifs

1.2.2. Les données judiciaires stockées dans des banques de données

Le casier judiciaire n'est pas le seul moyen d'accéder aux condamnations pénales prononcées contre des personnes. Les bases ou banques de données qui recueillent les décisions de justice, judiciaires ou administratives, sont également une source d'information dont l'usage peut être dévoyé de sa finalité première. La CNIL veille toutefois au grain. Pour la première fois, le 12 juillet 2011, la formation contentieuse de la CNIL a sanctionné un site Internet pour pratiques attentatoires au respect de la vie privée des personnes et au droit à l'oubli numérique pour avoir diffusé des décisions de justice non anonymisées[139]. En l'espèce, l'association LEXEEK, qui a pour objet d'œuvrer en faveur de la numérisation à la source des décisions de jurisprudence rendues par les juridictions françaises, avait mis en ligne une banque de données de décisions de jurisprudence nominatives, en libre accès. En vain, les plaignants avaient sollicité leur droit d'opposition auprès du responsable de l'association. La CNIL avait donc été saisie de plusieurs plaintes de particuliers ayant découvert que les décisions de justice les désignant étaient publiées sur le site Internet de LEXEEK, celles-ci pouvant être la source de préjudices moraux, professionnels… A titre d'exemple, la CNIL rapporte que l'un des plaignants s'est vu refuser un poste après que son potentiel employeur ait, *via* une recherche sur le moteur de Google, consulté une vieille décision judiciaire sur le site de LEXEEK, qui concernait des faits mineurs, remontant à plus de 12 ans.

A l'issue d'une mise en demeure infructueuse datant du 29 mai 2008[140], la Commission décide d'initier les poursuites à l'encontre de l'association. La CNIL estime notamment, que l'association LEXEEK s'est rendue responsable de graves violations à la disposition de l'article 38 de la loi du 6 janvier 1978, selon lequel « toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fasse l'objet d''un traitement ». C'est ce qui explique que, le 12 juillet 2011, la formation contentieuse de la CNIL ait sanctionné LEXEEK en la condamnant à payer une amende de 10.000 euros, à cesser la diffusion sur Internet de décisions de justice non anonymisées et à publier la décision par voie de presse. Enfin, la CNIL a dénoncé ces faits au Procureur de la République afin que des poursuites pénales puissent éventuellement être engagées à l'encontre de l'association.

[139] Délibération n°2011-238 de la formation restreinte prononçant une sanction pécuniaire et une injonction de cessation de traitement à l'encontre de l'association LEXEEK

[140] L'association indiquait avoir pris un certain nombre de mesures « visant à réduire l'occurrence de mentions nominatives désignant les parties dans les décisions produites, à réduire l'impact d'une éventuelle omission involontaire sur une personne concernée et à garantir un droit de suppression effectif », jugé insuffisant et inefficient par la CNIL, cf. Délibération n°2011-238

Dans les années 80, la CNIL avait été alertée sur le fait que les bases de données jurisprudentielles avaient parfois pour objet non pas la recherche de décisions présentant un intérêt juridique dans un domaine particulier, mais plutôt la recherche de l'ensemble des décisions de justice concernant une même personne. C'est pourquoi, dès 1985, la Commission rappelait que « les bases de données jurisprudentielles constituent, lorsqu'elles comportent l'identité des parties, des traitements automatisés d'informations nominatives au sens de l'article 5 de la loi du 6 janvier 1978[141] et doivent, à ce titre, être déclarées à la Commission »[142]. Toutefois, elle n'avait pas encore jugé indispensable l'anonymisation de ces bases de données.

Il faut attendre l'adoption d'une recommandation de 2001[143] relative à la diffusion de données personnelles sur Internet par les banques de données de jurisprudence. Celle-ci répond au souci de concilier cette diffusion avec la protection des personnes physiques, parties ou témoins au procès, citées dans ces décisions et d'assurer un juste équilibre entre le caractère public des décisions de justice et les droits et libertés des personnes concernées.

Cette réflexion est guidée par la volonté de prévenir les risques de détournement de finalité des bases de données jurisprudentielles qui peuvent se transformer en véritables fichiers de renseignements sur les personnes citées dans des décisions de justice.

La CNIL a attiré l'attention des éditeurs de bases de données de décisions de justice sur les conséquences de l'application de la loi du 6 janvier 1978 « informatique et libertés » lorsque leurs « produits » comportent le nom des parties : interdiction de mentionner les infractions et condamnations pénales, interdiction de faire apparaître, directement ou indirectement, les origines, les opinions politiques, philosophiques ou religieuses, les appartenances syndicales ou les mœurs des personnes, reconnaissance du droit de s'opposer, pour des raisons légitimes, à voir figurer son nom dans une décision de justice diffusée sur support numérique, droit de rectification en cas d'information inexacte.

Par ailleurs, elle a appelé l'attention des organismes de presse sur l'intérêt qui s'attacherait à une réflexion d'ordre déontologique sur la mise en ligne, sur des sites web en accès libre, de comptes rendus de procès ou de décisions de justice citant des personnes physiques parties ou témoins au procès. Dans sa recommandation, la CNIL a ainsi préconisé

[141] « Sont soumis à la présente loi les traitements de données à caractère personnel : 1° Dont le responsable est établi sur le territoire français. Le responsable d'un traitement qui exerce une activité sur le territoire français dans le cadre d'une installation, quelle que soit sa forme juridique, y est considéré comme établi ; 2° Dont le responsable, sans être établi sur le territoire français ou sur celui d'un autre État membre de la Communauté européenne, recourt à des moyens de traitement situés sur le territoire français, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur ce territoire ou sur celui d'un autre État membre de la Communauté européenne » art 5-I Loi du 6 janvier 1978.

[142] Délibération n°85-44 du 15 octobre 1985.

[143] Délibération n°01-057 du 29 novembre 2001 portant recommandation sur la diffusion de données personnelles sur Internet par les banques de données de jurisprudence.

l'anonymisation des décisions de justice librement accessibles sur Internet en demandant aux éditeurs de bases de données de s'abstenir d'y faire figurer le nom et l'adresse des parties ou des témoins au procès, quels que soient l'ordre et le degré de la juridiction et la nature du contentieux. Pour les personnes physiques parties à un procès, la CNIL estime que la mise en ligne de l'information peut conduire à une « peine d'affichage numérique ». La démarche est louable mais nous verrons que, d'un point de vue technique, l'anonymisation n'offre pas une garantie absolue.

En ce qui concerne le cas particulier des sites spécialisés en accès restreint (procédure d'abonnement préalable ou achat à la demande) et des CD-Roms payants de jurisprudence, la CNIL, tout en relevant que les restrictions d'accès à ces sources d'information paraissaient de nature à limiter les risques d'utilisation détournée de ces bases, a également estimé que les éditeurs de ces bases de données devraient s'abstenir, à l'avenir, d'y faire figurer l'adresse des parties au procès ou des témoins.

Selon le communiqué de la CNIL du 10 octobre 2011, la décision de sanction concernant l'association LEXEEK « traduit la ferme volonté de la CNIL de faire respecter cette recommandation protectrice de la vie privée des personnes et de garantir un véritable droit à l'oubli sur Internet ». Il s'agit d'une décision forte qui offre un moyen d'agir en amont pour la préservation de la vie privée et des données à caractère personnel. Le but de la mesure est d'éviter notamment le profilage. Elle comporte naturellement des limites lorsqu'il s'agit d'affaires qui ont été médiatisées dans la mesure où d'autres sources relaieront alors l'information mais c'est là le jeu normal du droit à l'information sur lequel nous reviendrons.

On observera que cette nouvelle offre de service d'accès aux décisions judiciaires court-circuite en partie le système du casier judiciaire qui avait été pensé pour éviter les dérives et les atteintes aux droits des personnes. Dès lors que des opérateurs privés ont compris qu'Internet leur offrait un nouveau marché, ils ont exploité ces technologies en faisant l'impasse sur une réflexion préalable liée aux droits des personnes concernées ce qui génère de nouveaux questionnements. L'intérêt de pouvoir accéder librement à la jurisprudence n'est pas à démontrer. Il doit cependant se faire dans le respect des droits des personnes concernées.

1.3. Les données relatives à l'état et à la situation personnelle et sociale de la personne

Le droit à l'oubli a-t-il une résonnance particulière au regard du droit des personnes et de la famille ? Peut-on jamais oublier ou plus précisément, faire oublier son état et sa famille ?

En effet, la perception commune du droit des personnes et de la famille est particulièrement liée à la question de l'état que l'on pense *a priori* immuable[144]. Il pourrait ainsi être envisagé que cet état ne soit pas aux prises des volontés et qu'il n'y ait pas de pouvoir ni de disposition sur les données personnelles qui le reflètent.

Pourtant, les caractéristiques de l'état des personnes et des relations familiales démontrent qu'ils sont aussi soumis aux interrogations actuelles sur les données personnelles. Il faut s'interroger sur le point de savoir si ces dernières peuvent être l'objet d'un droit à l'oubli permettant à l'individu de soustraire des relations sociales certains événements de sa vie personnelle. Envisager les différentes caractéristiques des données personnelles en matière de droit des personnes et de la famille permettra de comprendre la singularité de la problématique et de la pousser à son paroxysme.

Au titre de la première caractéristique, l'on peut souligner que subir son état ou sa famille n'est plus un élément déterminant du droit des personnes et de la famille du XXIème siècle. Les personnes veulent marquer leur volonté sur ces éléments fondamentaux qui va aussi les constituer. La protection de la volonté et de la manifestation des choix des personnes est devenue particulièrement importante en droit des personnes et de la famille. Le mouvement d'individualisation que connaît notre système juridique et social promeut l'individu dans son unicité, y compris dans sa famille.

Cette force est portée par les libertés individuelles et la protection des droits fondamentaux. Elle donne à la personne ce pouvoir à régir ses propres prérogatives juridiques même sur des éléments structurants comme l'identité ou les relations familiales. Il s'agit ainsi d'être actif à propos de son état et non pas de le subir. L'oubli « moderne » est ainsi visé dans cette situation selon laquelle un choix est fait de ne plus se souvenir, voire de soustraire à la mémoire de la personne certains événements et donc certaines données les concernant. L'oubli « moderne » serait ainsi diligenté soit par l'individu lui-même, soit par l'Etat qui gère l'ensemble des données. Il ne s'agit pas de viser la première définition de l'oubli qui est de ne pas se rappeler et qui vise un comportement constaté chez le sujet de droit. Dans ce dernier cas, il faudra tirer les conséquences de l'oubli : rappeler à l'individu ses obligations, voire le sanctionner comme lorsqu'il oublie de déclarer des revenus ou encore conduire à le protéger en prenant en considération les dangers liés à ces oublis. La démarche volontariste du sujet de droit suppose de déterminer comment elle pourrait prospérer. L'expression de la volonté peut-elle emporter, à elle seule, la soustraction des données relatives à l'état de la personne ?

[144] Cf. D. Gutmann, *Le sentiment d'identité*, Préf. F. Terré, LGDJ, 2000.

La volonté de la personne souhaitant agir de la sorte interroge. En effet, l'état de la personne concerne une situation pour laquelle la puissance régalienne intervient. Cette question de l'état de la personne et de la famille ne concerne pas que la personne elle-même mais aussi l'Etat et les tiers. La loi organise l'état des personnes et de la famille qui s'inscrit dans les relations sociales, qui permet d'identifier chaque sujet de droit. Ainsi, au titre de la deuxième caractéristique, il convient de souligner qu'en droit des personnes et de la famille les données personnelles ne sont pas « traitées » par les individus eux-mêmes ; c'est un service de l'Etat ou un organisme social qui gère ces données personnelles et répond à une fonction de police. Il faut alors être d'autant plus protecteur pour l'individu car il n'a pas la maîtrise du traitement des données.

Au-delà de cette protection, il faut aussi protéger ces données car elles sont importantes pour la compréhension des relations sociales. Par ailleurs, leur traitement informatique confère un aspect nouveau à la question. En effet, le système technique permet de garder leurs traces quand bien même la personne croit qu'il n'y a plus d'accès. La destruction d'un document papier original peut suffire à faire disparaître une donnée ; il n'en est rien quand le traitement est informatisé. Le contrôle devient d'autant plus délicat lorsque ces données personnelles sont administrées par des tiers[145].

Enfin, les données relatives à la personne et sa famille sont de diverses formes. La troisième caractéristique vise à distinguer deux natures des données personnelles. D'une part, des éléments factuels importants (naissance, identification du sexe, choix des prénoms et du nom de famille) sont obligatoirement relatés dans un acte juridique. Les conséquences juridiques de ces faits - détermination notamment de l'âge, du sexe ou de la filiation - sont telles que la transcription de l'événement est nécessairement dans un acte juridique encadré et protégé. Cette transcription permet d'investir l'individu de toute sa personnalité juridique, de l'intégrer dans sa famille et dans le groupe social. Certes, on pourra, selon les circonstances, modifier cette situation parce que l'événement factuel a évolué (l'enfant sera adopté, le sexe a changé) et il faut adapter les actes juridiques à ce changement. Mais les mécanismes juridiques sont particulièrement réglementés et limités. Toutes les données personnelles relatives à l'état des personnes ou de la famille n'ont pas cette force identitaire.

[145] Certaines informations pratiques concernant les mentions transcrites sur le registre de l'état civil ont été obtenues dans le cadre d'un entretien mené par un membre de l'équipe de recherche avec la responsable du service de l'état civil de la mairie de Rennes, le 14 janvier 2014.

D'autre part, les données personnelles visent aussi des éléments d'identité devant être connus pour déterminer les prérogatives de l'individu à l'égard de l'Etat et des organismes sociaux. Il s'agit par exemple de recenser les revenus de la personne, la composition de sa famille, la situation d'un éventuel danger supportée par un enfant, pour permettre que des droits sociaux ou un mécanisme de protection soient engagés. Ces données ne sont donc pas structurantes comme celles relatives à l'identité de la personne. Il est nécessaire de rattacher ces données à un événement particulier, lié à un fait social (comme la mise en danger) dont elles seront dépendantes. Les conséquences juridiques de ces données ne sont liées qu'à cet événement. Elles doivent s'effacer lorsque ce dernier disparaît.

La mise en œuvre d'un éventuel droit à l'oubli doit être déterminée en droit des personnes et de la famille en fonction de ces caractéristiques. Si le droit à l'oubli se définit comme « une prérogative qu'aurait chaque individu d'exiger que ne soit plus accessibles à tous certains événements ou certaines données le concernant (…), ce serait une forme de soustraction à la mémoire collective »[146]. En droit des personnes et de la famille, ce serait même une soustraction à sa propre mémoire, dictée par sa volonté ou permise par l'Etat détenteur des données personnelles.

A partir de l'étude des caractéristiques des données personnelles dans l'état des personnes et de la famille, une différence importante apparaît entre les données personnelles relatives à l'identité de la personne et celles relatives à sa situation personnelle et sociale.

Nous allons constater que cette caractéristique guide l'ensemble des dispositifs pour envisager le sort des données personnelles soit en raison de l'état de la personne soit en raison de sa situation personnelle et sociale. Dès lors la prise en considération d'un éventuel droit à l'oubli est différente dans ces deux hypothèses.

1.3.1. Le sort des données personnelles liées à l'état de la personne.

En droit des personnes et de la famille, les actes d'état civil déterminent l'identité de la personne. L'article 57 du Code civil énonce de manière limitative les mentions portées sur l'acte de naissance[147]. Dès lors que le sujet de droit souhaite agir, il doit nécessairement se confronter

[146] Cf. définition proposée en introduction.

[147] Article 57 Code civil : « L'acte de naissance énoncera le jour, l'heure et le lieu de la naissance, le sexe de l'enfant, les prénoms qui lui seront donnés, le nom de famille, suivi le cas échéant de la mention de la déclaration conjointe de ses parents quant au choix effectué, ainsi que les prénoms, noms, âges, professions et domiciles des père et mère et, s'il y a lieu, ceux du déclarant. Si les père et mère de l'enfant ou l'un d'eux ne sont pas désignés à l'officier de l'état civil, il ne sera fait sur les registres aucune mention à ce sujet.

à cet acte de naissance. Sa démarche sera motivée par une volonté d'oubli : oublier la naissance de son enfant, oublier le sexe qui lui a été attribué à la naissance. Est-ce que cela lui confère un droit à l'oubli ?

Les évolutions concernant les changements identitaires de la personne, comme le changement de nom, de sexe, sont mentionnées sur les registres qui gardent ainsi trace de l'identité initiale de la personne. Le droit à l'oubli qui consisterait en un effacement de cet événement pour un individu n'est pas possible en la matière.

La demande d'oubli, ne plus se souvenir de son état antérieur, motive bien la demande de l'intéressé. Cependant, elle n'est pas protégée par un droit à l'oubli : tout effacer ou rendre les informations relatives à son état antérieur totalement inaccessibles aux tiers, dans cette démarche de « faire oublier », ne sera pas envisageable eu égard aux actes d'état civil. D'une part, les registres initiaux gardent mention des différents éléments, seuls sont modifiés les actes transmis à la personne. D'autre part, les changements sont limités dans leur objet. Ainsi, lorsqu'un individu demande à ce qu'au moment de son changement de sexe, son acte d'état civil soit modifié mais que son acte de mariage le soit aussi, les juges refusent d'accéder à cette demande. L'acte de mariage ne sera pas modifié[148].

Le droit à l'oubli n'a pas de légitimité lorsqu'il s'agit de l'état de la personne car l'établissement de l'identité de la personne a une place très protégée dans le système juridique français. L'Etat garde trace de tous les événements identitaires car ils sont structurants pour la personne et pour son entourage. Si l'évolution de cet état est dorénavant admise, permettant ainsi de considérer que l'état n'est plus immuable, il existe toujours trace des étapes fondatrices de la personne[149]. L'individu ne peut pas se considérer comme étant propriétaire de ses données personnelles sur lesquelles il aurait un *abusus*, un pouvoir de disposer, absolu.

En revanche, le droit à une forme de « déconnexion » existe. A défaut d'être propriétaire de ses données personnelles, il doit pouvoir exercer ses libertés individuelles dont celle de changer d'état et que son état civil soit conforme avec celui-ci. La protection de l'individu est

---

Les prénoms de l'enfant sont choisis par ses père et mère. La femme qui a demandé le secret de son identité lors de l'accouchement peut faire connaître les prénoms qu'elle souhaite voir attribuer à l'enfant. A défaut ou lorsque les parents de celui-ci ne sont pas connus, l'officier de l'état civil choisit trois prénoms dont le dernier tient lieu de nom de famille à l'enfant. L'officier de l'état civil porte immédiatement sur l'acte de naissance les prénoms choisis. Tout prénom inscrit dans l'acte de naissance peut être choisi comme prénom usuel. (…) ».

[148] Décision Cour d'appel de Rennes 16 octobre 2012, Jurisdata 2012-023535, JCP N 2013, n°4, n°1009, note J.-D. Azincourt.

[149] Cf. aussi dans un domaine particulier, la demande d'effacer un nom d'un registre de baptême, acceptée en première instance (Tribunal Coutances 6 octobre 2011, non publié) et refusée en appel (CA Caen 10 septembre 2013, non publié) sur le fondement qu'en raison de la séparation de l'Eglise et l'Etat, la première est libre d'organiser les registres comme elle l'entend et que ces derniers ne sont pas publics. Il a été invoqué par l'Eglise que l'existence du baptême doit être toujours connue car c'est un sacrement que l'on ne peut recevoir deux fois. Il existe dans cette hypothèse un intérêt à garder la mémoire de cet événement.

principalement assurée par l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, que l'on retrouve au visa de nombreuses décisions relatives à l'état des personnes. Il convient à la personne de la protéger dans son « épanouissement personnel »[150]. Ce dernier impose un changement d'état ayant pour corollaire que les tiers ne puissent plus faire de lien entre l'ancien état et le nouveau. Le droit à cette « déconnexion » permet donc de reconnaître à l'individu une prérogative, un droit subjectif à ce que ses changements et ses choix ne soient pas connus par les tiers. C'est une manière aussi de protéger la personne qui ne subira pas d'ostracisme du fait de ces évolutions d'état (comme être classé comme ayant changé de sexe : l'acte d'état civil dont il peut se prévaloir mentionnera seulement son dernier état). Il ne faut retenir que l'état dont il souhaite se prévaloir.

Les tiers, qu'ils soient privés ou publics, n'ont pas la possibilité de consulter les actes initiaux. Ainsi en cas d'accouchement dans le secret, un acte de naissance initial est créé. Cependant, personne ne pourra avoir accès à cet acte initial ; il est considéré comme détruit. Pour l'enfant né dans le secret de l'identité de sa mère, un nouvel acte est créé à partir de cet acte initial (par exemple pour reprendre le jour de naissance) mais qui ne permettra pas de faire le lien avec l'acte établi le jour de la naissance de l'enfant. La déconnexion est totale entre cet acte initial et le nouvel acte. D'un point de vue technique, il existera ainsi une rupture entre les différents registres et actes que ce soit sous forme papier ou sous forme numérique.

Mais ce droit à une « déconnexion » comme la manifestation de la liberté de l'individu de pouvoir opposer son changement ou ses choix à l'égard de son état ou de celui de son enfant doit être envisagé dans la limite des droits des tiers. Il ne s'agit pas de considérer que l'individu aurait des obligations mais plutôt de prendre en considération les propres libertés et droits fondamentaux des tiers (privés ou publics). Le droit à une « déconnexion » n'est pas absolu. L'exemple du droit à l'accès à ses origines personnelles l'illustre.

Des parents, et dans les faits surtout la mère, peuvent, en effet, décider de ne pas créer de lien avec un enfant et marquer leur volonté d'oublier l'existence de cet enfant. Dans ce cas de figure, l'acte de naissance de l'enfant ne mentionnera pas l'identité pour les parents. Malgré cela, le lien pourra être reconstitué entre les parents et l'enfant : au moment de la naissance l'équipe médicale doit inciter la mère à laisser un certain nombre d'éléments et le conseil national d'accès aux origines permet de mettre en œuvre les recherches engagées par les parents et les enfants.

[150] J. Rochfeld, *Les grandes notions du droit privé,* PUF, Thémis droit, 2011, spéc. 1-15 et s.

Cependant ce lien ne pourra pas se réaliser par les actes d'état civil, ni par les données personnelles liées à l'état des personnes. Il se produira par des éléments complémentaires (faits relatés dans le dossier de l'enfant qui sera mis à sa disposition au moment de ses recherches). La reconstitution du lien peut s'avérer compliquée voire même impossible compte tenu de la situation, mais le système juridique lui accorde une place au nom des libertés individuelles et des droits fondamentaux venant limiter le désir de toute puissance d'un individu sur son état ou sur l'état de son enfant. L'organisation de cette aide pour la recherche de ses origines évite ainsi une condamnation de la France par la Cour européenne des droits de l'homme[151]. L'opposabilité d'un éventuel droit à l'oubli absolu ne pourrait pas prospérer. La prise en considération des données personnelles liées à la situation personnelle et sociale des individus suppose de prendre en considération d'autres enjeux.

1.3.2. Le sort des données personnelles liées à la situation personnelle et sociale de la personne

Il existe de nombreuses données concernant la vie privée de la personne, son identité, qui sont transmises dans les relations juridiques familiales et sociales. L'*e-administration* recourt au traitement informatisé de ces données personnelles. Le traitement informatisé des données apparaît nécessaire tant au regard de la dématérialisation générale des procédures que de la nécessité de créer des liens entre les institutions traitant la situation de personnes (importants pour les traitements et les contrôles sociaux, fiscaux et pénaux des personnes). La connaissance de ces données permet aussi un traitement de statistiques afin de travailler d'un point de vue prospectif pour d'éventuelles réformes.

Ce mouvement de dématérialisation est irrémédiable. L'Etat et les organismes sociaux et fiscaux utilisent eux-mêmes les réseaux d'Internet et les réseaux sociaux pour communiquer avec les usagers. Tout comme le « dépôt de données » sur Internet et les réseaux sociaux par les individus eux-mêmes, le traitement informatisé des données personnelles des usagers est utile et nécessaire.

Ainsi le traitement des données à caractère personnel est envisagé pour l'attribution et le suivi du revenu de solidarité active[152], pour les centres d'hébergement et de réinsertion

[151] Affaire X contre Italie, CEDH 25 septembre 2012, aff. Godelli contre Italie : l'Etat italien est condamné du fait d'une absence totale d'institution permettant de favoriser l'accès aux origines, cf. Rev. Droit de la famille n°3, mars 2013, A. Gouttenoire, « La famille dans la jurisprudence de la Cour européenne des droits de l'homme », spéc. n°24.
[152] Pour le RSA, il existe des dispositions expressément nommées « @RSA », art. R. 262-102 du Code de l'action sociale et des familles.

sociale[153] ou encore pour le traitement des données pour les mineurs en danger[154]. Il existe ainsi de nombreux registres ou fichiers informatiques contenant des données personnelles en vue de leur traitement pour permettre aux personnes, vulnérables ou pas, une prise en charge (prestations, aides, procédure d'alerte).

Ces données personnelles visent des données relatives à la situation personnelle et sociale de l'individu. Elles sont donc liées à un événement ou une situation particulière (comme le fait d'être sans revenus, être un mineur en danger, être en situation de demander un hébergement d'urgence). Elles sont donc totalement dépendantes de ces événements. Quel pouvoir faut-il reconnaître à l'individu sur ces données personnelles ? Compte tenu de leurs natures temporaires et dépendantes d'un événement particulier, il est nécessaire de reconnaître des prérogatives individuelles de la personne pour soustraire ces données à la connaissance des tiers en dehors du cadre légal imposant le traitement des données. En dehors de la nécessité pour l'administration et les organismes sociaux d'avoir recours à ces données, l'individu recouvre un pouvoir absolu sur le sort de ces dernières. Cela d'autant plus qu'elles ne s'opposent pas aux libertés individuelles des tiers.

Dans ces hypothèses, il existe un droit à l'oubli, c'est-à-dire l'exercice d'une prérogative au profit de l'individu manifestant ainsi sa maîtrise sur sa situation personnelle et sociale. Nous ne sommes pas dans une configuration relative à l'état de la personne mais à sa situation personnelle et sociale. Si la légitimité du droit à l'oubli est reconnue, il convient de déterminer si ce droit est déjà mis en œuvre. Les différentes dispositions du Code de l'action sociale et des familles organisant le traitement des données envisagent aussi les modalités de protection des prérogatives de l'individu. Plusieurs outils juridiques sont déterminés.

Non seulement le législateur anticipe la nécessité de rompre le lien avec la personne (anonymat, conservation temporaire des données, techniquement il est précisé l'utilisation aussi de cryptage informatique) mais en plus l'usager lui-même a un droit d'opposition et de contrôle (cf. traitement juridique et protection juridique *via* la CNIL). L'ensemble doit être respectueux des droits fondamentaux et des libertés individuelles, notamment eu égard au respect de la vie privée[155]. Les textes précisent aussi l'exigence de confidentialité, la référence au secret professionnel (dans certaines hypothèses les agents sont soumis expressément à ce secret par

[153] Le traitement des données pour l'hébergement est envisagé par les articles L. 345-4 du Code de l'action sociale et des familles.
[154] Le traitement des données pour les mineurs en danger par les articles L. et D. 226-3-7 du Code de l'action sociale et des familles.
[155] Par exemple, le contrôle et le transfert des données au profit de l'administration fiscale sont possibles à condition de respecter la vie privée des personnes et que l'atteinte soit légitime et proportionnée, cf. sur ce point L. Ayrault, « Droit fiscal européen des droits de l'homme : chronique de l'année 2013 », à propos de CEDH 14 mars 2013, aff. Bernh Larsen Holding contre Norvège, Rev droit fiscal, n° 10, mars 2014, n°201.

référence au code pénal). Enfin les modalités d'exploitation des données ne doivent être envisagées qu'en cas de nécessité. Par exemple, la loi sur la géolocalisation du 28 mars 2014 envisage que certaines informations de l'enquête ne peuvent pas être transmises, que les enregistrements seront détruits à la diligence du Procureur de la république qui devra organiser les opérations de destruction[156].

L'encadrement du traitement de ces données est donc essentiel pour permettre à l'Etat ou aux organismes sociaux de connaître des données personnelles et de les utiliser. Il permet de coordonner l'action sociale au profit des individus, de contrôler le versement des prestations ou la constitution de certains patrimoines en matière fiscale. Cependant, l'ingérence de l'Administration sera proportionnée à la finalité des droits ouverts au profit de la personne : l'information ne portera que sur le strict nécessaire, les données ne sont conservées que pour un temps limité. Ainsi, faute d'encadrement suffisamment précis, le Conseil Constitutionnel le 13 mars 2014 a censuré la constitution d'un fichier national d'un crédit à la consommation dans la loi relative à la consommation[157].

Ce droit à l'oubli est légitime. Il s'agit d'envisager un effacement total. Si techniquement, cet effacement s'avère compliqué, il convient que les connexions ne soient plus possibles, et cela sans aucune limite. C'est en cela que nous pouvons constater une différence fondamentale entre le sort des données personnelles liées à l'état de la personne et celle liée à sa situation personnelle ou sociale.

Cependant, il est certainement regrettable que les modalités de protection ne soient pas harmonisées ou parfois d'une sécurité toute relative dans l'hypothèse des données relatives à la situation personnelle et sociale de la personne. S'il devait être question d'un droit autonome à l'oubli, l'intérêt ne serait pas dans une reconnaissance d'un droit qui existe déjà. Au-delà du symbole de conférer une qualification unique et clairement identifiable, la reconnaissance d'un droit à l'oubli autonome devrait nécessairement s'accompagner d'un régime juridique harmonisé pour tous les effacements de données.

Ce régime doit nécessairement comprendre les règles de proportionnalités dans la transmission des données entre organismes, de confidentialité et de secret professionnel. Par ailleurs, un délai précis, voire commun à toutes les formes de traitement des données

[156] Loi 2014-372 du 28 mars 2014 relative à la géolocalisation, cf. nouveaux articles 230-40 Code pénal et art. 230-4 Code pénal.
[157] Décision Conseil Constitutionnel 2014-690 DC, Loi relative à la consommation, JORF du 18 mars 2014 page 5450, texte n° 2.

personnelles, doit être établi ainsi qu'une information et un contrôle sur les modalités de destruction que ce soit des destructions physiques ou informatiques.

2. LES ACTEURS

Pour identifier les contours d'un droit à l'oubli, il convient également d'en déterminer les bénéficiaires potentiels et ceux à qui ils sont susceptibles de l'opposer. Nous aborderons donc les créanciers (2.1) puis les débiteurs du droit à l'oubli (2.2).

2.1. Les créanciers : qui doit-on (ou veut-on) protéger ?

Toutes les personnes dont les données sont traitées devraient pouvoir bénéficier d'un droit à l'oubli. Il apparaît en outre que la qualité du créancier peut justifier une protection accrue face à certains débiteurs. C'est le cas du salarié ou du candidat à un emploi. C'est donc sur la base d'une approche large qu'il convient d'envisager les personnes éligibles au droit à l'oubli en mettant l'accent sur les exigences particulières requises à l'égard de certaines de ces personnes.

2.1.1. Approche large des personnes éligibles au droit à l'oubli

Il est tout d'abord à noter que, dans la proposition amendée de règlement, il est prévu, à l'article 17 §1 bis, que « l'application du paragraphe 1 dépend de la capacité du responsable du traitement à vérifier que la personne demandant l'effacement est la personne concernée ». Il conviendra de retenir une interprétation large de la disposition qui ne doit pas faire obstacle au droit des proches d'agir, notamment, en cas de décès de la personne concernée ou dans l'hypothèse d'une incapacité juridique. Cette restriction peut s'expliquer par la volonté d'éviter un détournement du droit à l'effacement par des tiers, par exemple, des concurrents commerciaux de la personne concernée, qui de cette manière, rendraient les informations relatives à la personne concernée moins visibles.

Dans la version d'origine, l'article 17 §1 évoquait le cas des personnes ayant rendu leurs données disponibles lorsqu'elles étaient enfants mais par crainte d'un traitement moins favorable des personnes autres que les mineurs, la Commission LIBE a souhaité supprimer cette précision. Aux Etats-Unis pourtant, la *erase law* (littéralement, loi gomme) de l'Etat de Californie, du 23 septembre 2013, entrée en vigueur en 2015[158], instaure au profit des jeunes

[158] http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568.

un droit à l'effacement des traces numériques laissées avant leur majorité, en obtenant sur simple demande au site concerné, un retrait des informations. D'une manière générale, les demandes de déréférencement effectuées par des personnes mineures au moment de la publication de l'information les concernant devraient être satisfaites.

La CNIL estime également nécessaire de prendre en compte « l'intérêt supérieur de l'enfant » dans les demandes de déréférencement adressées aux fournisseurs de services de moteur de recherche en s'appuyant notamment sur les exigences de la Charte des droits fondamentaux de l'Union européenne qui dispose que « dans tous les actes relatifs aux enfants, qu'ils soient accomplis par des autorités publiques ou des institutions privées, l'intérêt supérieur de l'enfant doit être une considération primordiale » (article 24)[159].

Si une approche large doit être préconisée, elle comporte tout de même des limites. En effet, à l'instar du concept du droit au respect de la vie privée, le champ d'un droit à l'oubli devrait être limité eu égard à la qualité des personnes et l'on songe, tout particulièrement, aux personnalités publiques[160]. Tout le monde se souvient de l'embarras de Lionel Jospin à l'évocation de sa jeunesse trotskyste. Ou encore du tollé provoqué, lors de sa candidature en 2000, par le rappel d'une arrestation de Georges W. Bush en état d'ébriété …24 ans auparavant. En outre, l'usage d'Internet brouille également la notion de personnage public. En effet, comme le soulignait Pierre Trudel, chercheur Canadien, « il y a sur Internet des situations dans lesquelles une personne est en position publique. On ne peut se mettre à publier son profil personnel sur Internet et exiger que cela n'emporte aucun risque »[161]. Cette position paraît particulièrement incompatible avec le droit à l'oubli. Cela conduit à se demander si la qualité de créancier n'est pas conditionnée par l'origine de la diffusion : Celui qui met en ligne des informations le concernant ne serait pas éligible au droit à l'oubli.

On voit immédiatement la limite d'une telle préconisation. Elle est double. Technique d'abord. Il faudrait être en mesure de prouver l'origine de la diffusion. Rationnelle ensuite. Cela empêcherait une personne ayant posté un profil à 15 ans de s'opposer à l'utilisation de ces données à 30 ans. Sans tomber dans les exemples les plus excessifs de photos compromettantes postées sur un réseau social, on peut imaginer des photos sur lesquelles la personne effectue une grimace par exemple, qui pourrait être ennuyeuse face à certains employeurs. Il nous semble toutefois que l'application du régime de protection des données personnelles permettrait

[159] CNIL, Droit au déréférencement, Les critères communs utilisés pour l'examen des plaintes, http://www.cnil.fr/fileadmin/documents/Vos_libertes/Droit_au_dereferencement-criteres.pdf, critère 3.
[160] B. Beignier, Vie privée et vie publique, sept. 1995, Légipresse p. 67 s..
[161] Trudel P., « Quelles limites à la googleisation des personnes ? » *in La sécurité de l'individu numérisé, Réflexions prospectives et internationales*, S. Lacour (dir.), L'Harmattan 2010, p.53.

de répondre de manière satisfaisante à cette problématique grâce, notamment, au régime de conservation des données ou au droit d'opposition par exemple mais nous reviendrons plus loin sur cette situation. En réalité, ce critère de la qualité de personnage public ou d'auteur de la diffusion de l'information n'est pas un critère satisfaisant. Ce qui compte, c'est l'intérêt légitime que le public a à connaître une information. Le principal angle d'appréciation est alors non plus subjectif mais téléologique et la CJUE l'a bien compris[162].

Pour autant, dans certains cas, le droit tient compte de la qualité de la personne pour reconnaître une forme de droit à l'oubli, c'est le cas par exemple des salariés vis-à-vis de l'employeur.

2.1.2. Illustration de la relativité des contours du droit à l'oubli : le cas des salariés

Les traitements de données à caractère personnel sont omniprésents pour les opérateurs économiques (réseaux internes et externes : *cloud computing, big data*, réseaux d'entreprises/intranet, base de données, etc …). Les finalités sont très diverses : recrutement, géolocalisation, vidéosurveillance, contrôle de l'accès aux locaux de l'entreprise, contrôle des horaires, contrôle de la messagerie électronique, etc. Ces traitements visent tous les interlocuteurs de l'entreprise, internes ou externes à celle-ci : salariés, clients, consommateurs, prospects, partenaires, etc.

La législation applicable au salarié tend à lui fournir un certain nombre de garanties face à l'employeur. Or, certaines dispositions du droit du travail consacre une forme de droit à l'oubli qui se manifeste à chacune des étapes de la vie professionnelle d'un salarié, de son embauche à son départ de l'entreprise. Sur ce point, si la tenue d'un registre du personnel est obligatoire, celle de dossiers individuels du personnel ne l'est pas. Pour autant, ces dossiers constituent le plus souvent pour l'employeur le film de la vie professionnelle et parfois extraprofessionnelle de son salarié. En effet, ont vocation à figurer dans ces dossiers les faits marquants de sa carrière professionnelle, par exemple l'embauche, la modification du contrat de travail, les dates d'arrêt pour absence et de reprise du travail, la ou les période(s) de grossesse, les incidents de parcours (notamment disciplinaires).

Les TIC ont contribué à une nouvelle approche des relations professionnelles. Elles ont généré des tensions croissantes entre employeurs et salariés et ces tensions s'inscrivent dans un

[162] Aff. C-131/12 Google Spain c/ AEPD 13 mai 2014, *infra*.

mouvement plus large de remise en cause de la frontière vie professionnelle et vie privée. Les TIC menacent la vie privée du salarié, avant même qu'il soit embauché. La décision de recrutement peut aujourd'hui se fonder sur **toutes les traces numériques** que le candidat à l'emploi a disséminées sur Internet.

Les entreprises sont soumises aux dispositions de la loi Informatique et libertés. Elles doivent, par conséquent, composer avec l'impératif de protection des données personnelles. Il est permis de considérer qu'elles constituent un levier fondamental de l'effectivité d'une politique de protection des données personnelles.

D'une part, la gestion du risque interne, en matière de protection des données personnelles, par les entreprises suppose une parfaite maîtrise de la loi Informatique et Libertés et une sensibilisation des salariés aux problématiques liées à la protection des données personnelles. L'élaboration d'une culture d'entreprise intégrant l'impératif de protection des données personnelles passe notamment par la formation et l'information des salariés. Les chartes de protection des données personnelles, les codes informatiques et les codes éthiques relatifs à la sécurité des données personnelles permettent de formaliser les bonnes pratiques en les uniformisant et en les diffusant dans l'entreprise. Ceci posé, le degré d'applicabilité de telles pratiques par les collaborateurs se trouve renforcé.

D'autre part, la gestion du risque interne, en matière de protection des données personnelles, par les entreprises suppose la mise en place de dispositifs de surveillance des salariés. Ces dispositifs sont très encadrés. Ils doivent être pertinents et proportionnés au but recherché. Ils doivent s'opérer dans le respect de la vie privée des salariés et dans le respect des données personnelles ainsi collectées.

C'est donc à tous les stades de la vie salariale qu'il convient d'intégrer le droit à l'oubli du salarié, de l'embauche à la rupture du contrat de travail.

2.1.2.1. Au stade de l'embauche

L'« e-recrutement » est aujourd'hui une réalité[163]. Sachant que tout ce qui est publié sur Internet est indexé par les moteurs de recherche, les chargés de recrutement ou les cabinets de recrutement, de plus en plus, « googelisent » les candidats[164]. En cherchant sur un moteur de recherche le nom d'un candidat, ils ont accès à tout ce qui a été publié par et sur le candidat. Il suffit alors aux recruteurs d'accéder aux informations publiées sur ces réseaux pour en

[163] J-Ph. Tricoit, « Recrutement, rupture du contrat de travail et TIC », JCP S 2013, 1381.
[164] V. Retour sur le rapport « L'oubli numérique est-il de droit face à une mémoire numérique illimitée ? » du 25 mai 2010, rédigé par le groupe « Droit à l'oubli » de Cyberlex. Colloque organisé par Cyberlex – Lundi 6 décembre 2010 – Revue Lamy Droit de l'Immatériel 2011 – n°71.

apprendre beaucoup plus sur un candidat que ce qu'il aurait été possible *via* le simple entretien d'embauche, et ce bien en amont de l'entretien[165].

Cependant, ce type de recrutement est susceptible de heurter le Code du travail. Il importe de souligner que les principes gouvernant tout recrutement (non-discrimination – art.L.1132-1 C.trav, transparence – art.L.1221-8 et s C.trav, pertinence – art.L.1221-6 C.trav et confidentialité – art.L.1221-8 C.trav) régissent également l'e-recrutement.

L'article L.1221-8 du Code du travail dispose que « le candidat à un emploi est expressément informé, préalablement à leur mise en œuvre, des méthodes et techniques d'aide au recrutement utilisées à son égard ». Or il est très probable que cela ne soit jamais le cas. Il en est de même de l'article L.1221-9 du code du travail qui dispose qu' « aucune information concernant personnellement un candidat à un emploi ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance ».

Mais, en réalité, l'application de ces articles est singulièrement limitée. Comment en effet un candidat évincé pourra-t-il prouver qu'un recruteur a obtenu des informations sur les réseaux sociaux ? Comment pourra-t-il prouver que ces informations sont contraires à l'article L.1221-6 du code du travail qui prévoit que « les informations demandées, sous quelque forme que ce soit, au candidat à un emploi ne peuvent avoir comme finalité que d'apprécier sa capacité à occuper l'emploi proposé ou ses aptitudes professionnelles […]. Ces informations doivent présenter un lien direct et nécessaire avec l'emploi proposé ou avec l'évaluation des aptitudes professionnelles […] » ?

Dans le prolongement, le recruteur peut commettre un acte discriminatoire. L'article L. 1132-1 du code du travail dispose qu' « aucune personne ne peut être écartée d'une procédure de recrutement […] ou faire l'objet d'une mesure discriminatoire, directe ou indirecte ». Le non-respect de cette disposition entraîne l'engagement de la responsabilité pénale de l'intéressé. L'article 225-1 du code pénal dresse une longue liste de critères discriminatoires. Ainsi, « constitue une discrimination toute distinction opérée entre les personnes physiques à raison de leur origine, de leur sexe, de leur situation de famille, de leur grossesse, de leur apparence physique, de leur patronyme, de leur état de santé, de leur handicap, de leurs caractéristiques génétiques, de leurs mœurs, de leur orientation sexuelle, de leur âge, de leurs opinions politiques, de leurs activités syndicales, de leur appartenance ou de leur non-appartenance, vraie ou supposée, à une ethnie, une nation, une race ou une religion déterminée ». Et il s'avère que

[165] E. Walle et S. Savaïdes, « L'e-réputation sous le prisme du droit du travail », Gaz. Pal 15 octobre 2011, n°288, p.26.

ces données personnelles sont susceptibles de se retrouver sur la page personnelle d'une personne membre d'un réseau social.

Si en France la pratique du « e-recrutement » *via* les réseaux sociaux commence à voir le jour, aux Etats-Unis, elle est déjà bien présente[166]. Parfois même, les entreprises et autres recruteurs ont un recours exclusif ou quasi exclusif aux réseaux sociaux. Cela suscite nombre de questions transposables à la réalité française. Selon une étude du magazine Workforce management, l'usage exclusif de Twitter et de LinkedIn dans le recrutement augmente le risque de discrimination. Ainsi, selon cette étude, seulement 5 % des usagers de LinkedIn sont noirs et 2 % sont hispaniques. De plus, de telles pratiques permettent de ne toucher qu'un nombre limité de candidats, principalement âgés entre 20 et 40 ans et masculins. Les études statistiques tendent à prouver que cette pratique du recrutement par les réseaux sociaux pourrait être discriminante pour certaines catégories de personnes, comme les personnes de plus de quarante ans par exemple.

En tout état de cause, la question se pose de savoir où se situe la frontière entre un regard sur les données et le fait de retenir ces données pour attribuer un poste ou une promotion. En pratique, il sera difficile pour un candidat à une offre d'emploi de prouver d'une part que le recruteur a procédé à un examen de ses données personnelles et d'autre part qu'elles ont servi de motif de non recrutement ou de non promotion.

Pour contrer ce phénomène, certains cabinets de recrutement ont signé des chartes de bonnes pratiques en la matière où ils s'engagent à ne pas se servir des réseaux sociaux. Ainsi en est-il par exemple des cabinets de recrutement membres de l'association « A compétences égales » dont les partenaires sont, entre autres, l'Association Nationale des Directions des Ressources Humaines (ANDRH), les cabinets Syntec Conseil en recrutement, Viadéo (réseau social dit professionnel), le Mouvement des Entreprises de France (MEDEF), l'Association Pour l'Emploi des Cadres (APEC)…[167].

Cette charte, dont la faiblesse réside dans le fait que son application ne dépend que du bon vouloir des signataires[168], insiste sur plusieurs points dont la limitation du recours aux réseaux sociaux dits personnels à la seule diffusion d'une offre d'emploi, la non utilisation des

[166] En 2010, 47% des DRH français recrutent *via* Facebook. 45% DRH américains. Et 38% des DRH reconnaissent rejeter un CV en raison des données mises à disposition sur les réseaux sociaux.
[167] Voir sur ce point : Charte « réseaux sociaux, Internet, vie privée et recrutement » du 14 novembre 2010. - M.Berguig et C.Thiérache, « L'oubli numérique est-il de droit face à une mémoire numérique illimitée ? », Cyberlex, rapport du 25 mai 2010, Revue Lamy Droit de l'Immatériel 2010 – n°62.
[168] Voir *infra.*

moteurs de recherche et des réseaux sociaux comme outil d'enquête pour collecter ou prendre connaissance d'informations d'ordre personnel même si elles sont rendues accessibles par les utilisateurs eux-mêmes ou encore la sensibilisation et la formation des recruteurs sur la nécessité de ne pas collecter ni tenir compte de telles informations.

Il importe de noter également l'existence de la charte du droit à l'oubli dans les sites collaboratifs et les moteurs de recherche du 13 octobre 2010 (Benchmark Groupe – Copainsdavant, Pages Jaunes – 123 people, Skyrock, Microsoft France – MSN, Windows live, Bing)[169].

A l'heure actuelle, il semble que seuls quelques cabinets de conseil en recrutement se soient engagés dans ce type de charte. Pour prendre l'exemple des cabinets de conseil en recrutement Syntec, ces derniers s'engagent à ne pas retenir au moment du recrutement ce qui a pu être vu sur les réseaux sociaux. Ainsi, si une présélection est effectuée par les chargés de recrutement, le consultant n'en a pas connaissance et son choix se fait sans *a priori* au moment du face à face avec le candidat.

La CNIL considère que l'utilisation d'annonces qui ne correspondraient pas à un poste à pourvoir mais auraient pour seul objet de constituer un fichier de candidatures en application des dispositions de l'article 25 de la loi du 6 janvier 1978 constituerait une collecte de données, par tout moyen frauduleux, déloyal ou illicite, dès lors interdite[170].

Qu'en est-il des informations transmises au recruteur ? Comme le précise le guide des bonnes pratiques de la CNIL, établi en 2013, en cas d'issue négative, le recruteur est tenu d'informer le candidat qu'il souhaite conserver son dossier afin de lui laisser la possibilité d'en demander la destruction. Si un candidat ne demande pas la destruction de son dossier, les données sont automatiquement détruites deux ans après le dernier contact. En tout état de cause, le droit à l'oubli numérique est composé du droit à l'anonymat, du droit de demander l'accès, la modification et la suppression de données et contenus concernant un individu[171].

La phase préalable du recrutement mérite également attention dans la mesure où elle entraîne le plus souvent un échange de documents (descriptif du poste vacant ou créé, lettre de candidature du salarié, curriculum vitae, etc…). Il peut être utile pour l'employeur de les conserver au moins pendant les débuts professionnels du salarié dans l'entreprise. Toutefois, à ce stade de la naissance de la relation de travail, le droit à l'oubli a vocation à trouver sa place

[169] **C**.Thiérache, « Le droit à l'oubli numérique : un essai qui reste à transformer – Charte du droit à l'oubli dans les sites collaboratifs et les moteurs de recherche du 13 octobre 2010 », Revue Lamy Droit de l'immatériel 2011 – n°67.
[170] CNIL, délib n°02-017, 21 mars 2001.
[171] E.Walle et S.Savaïdes, op.cit, p30.

dans la mesure où les opérations de recrutement sont guidées par plusieurs règles protectrices contre les atteintes à la vie privée et aux libertés individuelles. Ainsi, selon la jurisprudence de la Cour de cassation, une condamnation pénale antérieure n'a pas à être mentionnée lors de l'embauche[172]. D'une manière générale, le législateur ne contraint pas l'employeur à vérifier les antécédents judiciaires d'un candidat à l'emploi. Cependant, le législateur est intervenu dans certaines professions en prévoyant que « nul ne peut être employé par une entreprise de surveillance, de gardiennage et de transport de fonds, s'il a fait l'objet d'une sanction disciplinaire ou d'une condamnation à une peine correctionnelle ou criminelle, avec ou sans sursis, devenue définitive, pour agissements contraires à l'honneur, à la probité ou aux bonnes mœurs ou pour atteinte à la sécurité des personnes et des biens »[173]. L'employeur est donc tenu de s'enquérir de la probité du candidat à l'emploi et rien ne l'empêche de demander au salarié de fournir un extrait de son casier judiciaire qui lui permettra d'accéder aux informations offertes par le bulletin n°3[174].

La réforme du cadre juridique de la protection des données personnelles dans l'UE - proposition de règlement 2012 et la proposition de résolution de 2014 - s'accompagne d'avancées notables : droit à l'effacement, droit d'accès des personnes à leurs données, droit d'opposition spécifique au profilage. Ces mesures produiront des conséquences importantes sur la gestion des risques internes à l'entreprise, notamment en matière de contrôle et de surveillance de l'activité des salariés[175].

Ainsi, s'agissant du droit d'opposition spécifique au profilage (amendement 33, projet de règlement, considérant 58), il permettra à la personne de s'opposer à ce que ses données soient collectées aux fins d'évaluer certains aspects personnels propres à une personne physique ou d'analyser ou prévoir en particulier le rendement professionnel de celle-ci, sa situation économique, sa localisation, son état de santé, ses préférences personnelles, sa fiabilité ou son comportement. De plus, le profilage ne doit pas conduire à des discriminations fondées sur l'origine raciale ou ethnique, les opinions politiques, la religion ou les croyances, l'appartenance syndicale, l'orientation sexuelle ou l'identité de genre. En droit interne, fondées sur les articles L.1132-1 et suivants, les discriminations prohibées visent l'ensemble des actes

[172] Cass. soc., 25 avril 1990, RJS 1990, n°450.
[173] Loi n°83-629 du 12 juillet 1983 concernant les activités privées de surveillance, de gardiennage et de transport de fonds, complétée par D. n°86-1058 du 26 septembre 1986.
[174] Voir *supra*.
[175] Sur ce point voir E. Bailly et C. Le Corre., « L'entreprise et la protection des données personnelles », Revue Lamy Droit des affaires, 2013, n°87. - L. Barrau et A. Tessonneau., « Protection des données personnelles et risques juridiques pour l'entreprise, Economie et Management », n°147, Avril 2013, p24. - E. Geffray., » Projet de règlement sur les données numériques. Quelles conséquences pour les personnes concernées et l'entreprise ? », Revue Lamy Droit civil, 2013, n°100. - J-E. Ray., Actualité des TIC, Dr. soc 2013, p978.

relatifs à la relation de travail (le recrutement, la formation, les décisions d'affectation, de promotion, de mutation, la sanction du salarié, le licenciement du salarié).

La mise en œuvre de ces mesures-phares risque néanmoins de se heurter à des difficultés pratiques qu'il conviendra de résoudre au fil du temps. En tout état de cause, il serait prudent que les entreprises anticipent les changements impliqués par cette réforme très attendue, en procédant notamment à des analyses des risques que les traitements réalisés sont susceptibles d'engendrer.

2.1.2.2. Au stade de l'exécution de la relation de travail

Au stade de l'exécution de la relation de travail, le droit à l'oubli se manifeste à l'occasion de l'exercice du pouvoir disciplinaire de l'employeur. En effet, afin de garantir la bonne marche de l'entreprise, il est classiquement reconnu à l'employeur un pouvoir de direction et un pouvoir disciplinaire qui l'autorise à sanctionner le salarié pour son comportement fautif (C.trav., art. L.1331-1 et s). La constatation d'un tel agissement se fait lors du contrôle et de la surveillance par l'employeur de la bonne exécution du travail au sein de son entreprise. L'évolution de ce droit de contrôle et de surveillance a été marquée par un double mouvement législatif et jurisprudentiel au centre duquel se situe la protection des droits fondamentaux et des libertés individuelles et collectives des salariés. A l'origine de cette évolution, on trouve la généralisation des technologies de l'information et de la communication qui offrent un large éventail de procédés de contrôle et de surveillance : contrôle par autocommutateurs (usage du téléphone, productivité), contrôle par système d'écoutes téléphoniques, contrôle par vidéosurveillance, contrôle par l'outil informatique – cybersurveillance (traçage, contrôle des flux et des volumes, des temps de connexion). Il importe de rappeler sur ce point que la loi Informatique et libertés exige de tout employeur mettant en place un fichier informatique, c'est-à-dire un « traitement automatisé de données à caractère personnel », de faire une déclaration préalable à la CNIL. Dans le prolongement, la CNIL exige la destruction de plusieurs données informatiques concernant les salariés au-delà d'un certain délai. Cela concerne, par exemple, les enregistrements des auto-commutateurs (conduisant à répertorier les numéros de téléphone appelés par les salariés et ayant pour finalité de maîtriser les coûts de facturation) dont la durée de conservation est fixée à 6 mois, les badges d'entrée et de sortie des salariés dont la durée de conservation est fixée à 3 mois, les enregistrements de la pointeuse ou le traitement informatique remplaçant la pointeuse dont la durée de conservation est fixée à 1 an. Force est de convenir que de telles règles relatives à

l'archivage et à la destruction de documents et données informatiques contribuent d'une certaine manière à l'affirmation d'un droit à l'oubli dans l'entreprise.

Il est loisible de dresser un constat identique lors de l'examen des garanties offertes au salarié dans le cadre de la procédure disciplinaire. D'une part, aux termes de l'article L.1332-4 du Code du travail, « aucun fait fautif ne peut donner lieu à lui seul à l'engagement de poursuites disciplinaires au-delà d'un délai de deux mois à compter du jour où l'employeur en a eu connaissance, à moins que ce fait ait donné lieu dans le même délai à l'exercice de poursuites pénales ». L'action disciplinaire est ainsi soumise à un délai de prescription extrêmement court. L'employeur dispose en effet de deux mois à compter de la connaissance exacte des faits fautifs pour engager les poursuites, c'est-à-dire convoquer le salarié à l'entretien préalable. D'autre part, aux termes de l'article L.1332-5 du Code du travail, « aucune sanction antérieure de plus de trois ans à l'engagement des poursuites disciplinaires ne peut être invoquée à l'appui d'une nouvelle sanction ». Concrètement, un salarié ne peut être sanctionné deux fois pour les mêmes faits fautifs. Mais l'employeur peut parfaitement, lorsque les agissements ou omissions de même nature se répètent (« récidive disciplinaire »), tenir compte des fautes antérieures pour sanctionner plus sévèrement la plus récemment commise. L'article L.1332-5 limite cependant cette possibilité en interdisant à l'employeur de prendre en considération les sanctions prononcées plus de trois ans avant l'engagement d'une nouvelle action disciplinaire. A la différence de quelques lois d'amnistie consécutives aux élections présidentielles de 1981, 1988, 1995 et 2002 qui ont effacé des sanctions disciplinaires dans l'entreprise, cette disposition élabore un mécanisme qui s'apparente à une sorte d'amnistie permanente puisqu'il est interdit à l'employeur de tenir compte d'une sanction prononcée il y a plus de trois ans pour réprimer plus sévèrement une nouvelle faute, quand bien même celle-ci serait de même nature que l'agissement antérieurement sanctionné.

Précisons que le dernier texte relatif à l'amnistie en droit du travail est la loi du 6 août 2002. Elle comportait, comme les précédentes lois d'amnistie, des mesures de plein droit et des mesures individuelles. Caractérisée par un nombre accru d'infractions exclues de l'amnistie, elle fut qualifiée de « droit à l'oubli limité ». Plus précisément, à l'instar des autres lois d'amnistie, cette loi prévoyait une amnistie propre au monde du travail et traitait spécifiquement de l'amnistie des sanctions disciplinaires ou professionnelles. Le texte concernait les fautes disciplinaires et professionnelles commises avant le 17 mai 2002 et les faits retenus ou susceptibles d'être retenus comme motifs de sanctions prononcées par l'employeur commis avant le 17 mai 2002. Classiquement, il convenait alors de distinguer deux hypothèses. La

première concernait une sanction disciplinaire d'ores et déjà prononcée. Elle était amnistiée. Par conséquent, il ne pouvait plus y être fait référence et elle ne pouvait pas être conservée dans un quelconque dossier. La sanction était réputée n'avoir jamais existé. La seconde hypothèse concernait l'amnistie des faits fautifs. Aucune sanction ne pouvait être infligée au salarié pour ces faits dans la mesure où la procédure ne pouvait plus être engagée ou ne pouvait pas être menée à son terme. En tout état de cause, les employeurs étaient obligés de purger les dossiers des salariés qui ne devaient contenir aucune référence aux sanctions amnistiées. Le droit à l'oubli se manifestait alors de deux manières. D'une part, les lettres de sanction devaient être ôtées des dossiers des salariés et détruites dans la mesure où il ne pouvait en être gardé une trace. La sanction disciplinaire devait disparaître mais il pouvait être conservé une trace des faits ayant conduit à la sanction (ex : retards : sanctions fondées sur les retards du salarié sont supprimées mais l'employeur peut conserver au dossier les feuilles de pointage). D'autre part, l'employeur devait vérifier qu'il n'y avait aucun document faisant référence à des sanctions amnistiées dans l'ensemble de ses dossiers. Les sanctions devaient être supprimées des dossiers papier détenus au sein de l'entreprise mais également des fichiers informatiques, des microfiches, des archives de la société. L'inspecteur du travail devait veiller à la bonne réalisation de cette purge des dossiers disciplinaires.

2.1.2.3. Au stade de la rupture de la relation de travail

Au stade de la rupture de la relation de travail, le droit à l'oubli se manifeste par l'obligation pour l'employeur de détruire des documents et données informatiques, étant admis que l'archivage et la conservation des archives constituent des risques potentiels pour le droit à l'oubli. Sur ce point, il importe de noter que la CNIL exige la destruction de données informatiques concernant les salariés au-delà de la période d'emploi[176]. C'est le cas s'agissant des données destinées à la gestion administrative du personnel, des données destinées à la mise à disposition des personnels d'outils informatiques et enfin des données destinées à la gestion des carrières et de la mobilité.

Il faut préciser que si l'employeur souhaite garder l'information pour un délai plus long que celui indiqué ci-dessus, il est tenu de faire une demande à la CNIL et d'apporter les justificatifs correspondants.

[176] Délib. CNIL n°2005-002, 13 janvier 2005.

Il existe également un système de plainte en ligne mis en place par la CNIL concernant les problèmes de suppression des données personnelles sur Internet. Cependant, dans la mesure où les possibilités de duplication des contenus publiées sur Internet sont infinies, comment être sûr qu'une information mise en ligne sur Internet et pour laquelle une personne aurait fait valoir son droit à l'oubli numérique soit réellement supprimée ? Il existe toujours un risque qu'une information resurgisse.

L'étude permet de comprendre que le droit à l'oubli est difficilement envisageable comme un droit autonome. C'est ici l'environnement particulier dans lequel sont susceptibles d'être utilisées les données qui justifient des mesures particulières. Elles sont fondées sur les droits fondamentaux de la personne mais d'une manière somme toute relative puisque les restrictions ne sont pas strictement liées à la nature des données et au type d'usage qui en est fait mais également à la qualité des personnes concernées : salarié d'une part, employeur de l'autre.

L'étude permet également de saisir que dans ce contexte spécifique, toute la question réside dans l'effectivité de la mise en œuvre du droit à l'oubli numérique dans l'entreprise.

2.2. Les débiteurs du droit à l'oubli

D'une manière générale, les débiteurs d'un droit à l'oubli devraient être tous ceux qui ont eu accès à des données, quelle qu'elles soient, concernant une personne, qui qu'elle soit et qui « font quelque chose avec ces données ». La formulation est familière. Elle est pauvre. On pourrait être tenté de la remplacer par une autre par exemple, les débiteurs sont ceux qui « exploitent les données personnelles », mais il faudrait alors s'entendre sur la notion d'exploitation. Exploiter est-il conserver par exemple. Nous ne le pensons pas. De fait, il est extrêmement difficile de définir le débiteur d'un droit à l'oubli sans se référer au vocabulaire utilisé dans les textes organisant la protection des données à caractère personnel tant sa portée semble coïncider avec les exigences du droit à l'oubli. Si ce droit devait être consacré, il devrait pouvoir être opposable à tous ceux qui entrent dans la catégorie des « responsables de traitement ». Les débiteurs pourraient donc bien être les opérateurs qui effectuent un traitement de données personnelles.

Naturellement, la définition donnée du responsable de traitement est large et l'on doit tout de même se demander si elle embrasse exactement la catégorie des débiteurs d'un droit à l'oubli.

Il résulte de l'article 2 de la loi de 1978 qu'un **traitement** de données à caractère personnel correspond à « toute opération ou tout ensemble d'opérations portant sur (des données à caractère personnel), quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ». L'article 4 §3 de la proposition de règlement définit le traitement de données à caractère personnel comme « toute opération ou ensemble d'opérations effectuée(s) ou non à l'aide de procédés automatisés, et appliquée(s) à des données à caractère personnel, telle(s) que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que l'effacement ou la destruction ». Le changement n'est pas flagrant.

Cette définition constitue le préalable nécessaire à la compréhension de la notion de **responsable de traitement** qui, selon l'article 3 de la loi du 6 janvier 1978, est « sauf désignation expresse par les dispositions législatives ou réglementaires relatives (au) traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens ». La proposition de règlement définit, quant à elle, le responsable du traitement comme « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités, les conditions et les moyens du traitement de données à caractère personnel ; lorsque les finalités, les conditions et les moyens du traitement sont déterminés par le droit de l'Union ou la législation d'un État membre, le responsable du traitement peut être désigné, ou les critères spécifiques applicables pour le désigner peuvent être fixés, par le droit de l'Union ou par la législation d'un État membre » (article 4 §5).

La loi et la proposition de règlement envisagent en outre la possibilité de sous-traiter un traitement de données à caractère personnel. Le sous-traitant est défini comme « toute personne traitant des données à caractère personnel pour le compte du responsable du traitement »[177]. La sous-traitance est une modalité de traitement très répandue ce qui n'est pas sans inconvénient du point de vue de la responsabilité. En effet, au regard de la loi de 1978, un sous-traitant n'a pas la maîtrise des finalités et des moyens du traitement. Il en résulte qu'un traitement sous-traité demeure sous la responsabilité de l'organisme qui a décidé de recourir à un sous-traitant.

[177] Article 35 §2 de la loi. Article 4 § 6 de la proposition qui précise simplement la qualité des personnes visées qui peut être « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ».

Les seules obligations assumées par le sous-traitant sont une obligation de sécurité et une obligation de confidentialité.

La définition du responsable de traitement étant fournie, est-elle susceptible de couvrir tous les débiteurs potentiels d'un droit à l'oubli. La question se pose avec une acuité toute particulière face aux journalistes par exemple, aux archivistes ou encore aux scientifiques. Mais à leur égard, il existe dans le régime de protection des données personnelles des dispositions dérogatoires eu égard à la finalité du traitement qu'ils opèrent. Ils entrent donc *a priori* dans une catégorie à part de responsable de traitement. La question se pose également de façon sans doute plus pertinente pour les acteurs d'Internet et tout spécialement les intermédiaires, très visibles, donc plus faciles à actionner. Dans l'affaire Google Spain / AEPD en date du 13 mai 2014[178] sur laquelle nous reviendrons, l'avocat général dans ses conclusions, faisait remarquer que « toute personne lisant aujourd'hui un journal sur une tablette ou suivant un média social sur un smartphone apparaît comme effectuant un traitement de données à caractère personnel avec des moyens automatisés, et pourrait potentiellement relever du champ d'application de la directive dans la mesure où cette activité sort du cadre strictement personnel »[179].

« Dans l'environnement actuel, les définitions larges que reçoivent les données à caractère personnel, le traitement des données à caractère personnel et le responsable du traitement sont de nature à couvrir une série d'ampleur inédite de nouvelles situations factuelles liées aux évolutions technologiques. Cela s'explique par le fait que la plupart, si ce n'est la totalité des sites Internet et des fichiers qui y sont accessibles comportent des données à caractère personnel, telles que des noms de personnes physiques vivantes. Aussi incombe-t-il à la Cour d'appliquer une règle de raison, autrement dit le principe de proportionnalité, en interprétant la portée de la directive, de sorte à éviter la survenance de conséquences juridiques déraisonnables et excessives ». C'est l'approche que la CJUE avait consacrée dans l'arrêt Lindqvist du 6 novembre 2003[180], dans lequel elle avait rejeté une interprétation qui aurait pu conduire à conférer un champ d'application d'une ampleur déraisonnable à l'article 25 de la directive en ce qui concerne le transfert de données à caractère personnel vers des pays tiers dans le contexte d'Internet.

Pour l'avocat général, il convient donc « de dégager un équilibre correct, raisonnable et proportionné entre la protection des données à caractère personnel, l'interprétation cohérente des objectifs de la société de l'information, et les intérêts légitimes des opérateurs économiques

[178] CJUE 13 mai 2014, aff. C-131/12, JCP G 2014, p. 768, note L. Marino ; JCP E 2014, p. 1327, note G. Busseuil ; JCP E 2014, p. 1326, note M. Griguer.
[179] Aff. C-131/12, concl. Avocat général Niilo Jääskinen, §29.
[180] CJUE 6 novembre 2003, affaire C-101/01, Bodil *Lindqvist*,.

et des internautes au sens large»[181] et cela passe notamment par une identification des opérateurs d'Internet.

D'une manière générale, les services proposés sur Internet peuvent être source d'atteintes dont la réparation suppose la mise en œuvre de la responsabilité de son auteur. Le régime de responsabilité pénale ou civile applicable à ces activités a considérablement évolué au cours de ces dernières années. La multiplication des conflits mettant en cause les acteurs du Net, et tout spécialement les fournisseurs intermédiaires, a conduit à l'adoption de la directive communautaire n° 2000/31/CE du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (directive sur le commerce électronique), dont la section 4 est précisément consacrée à « la responsabilité des prestataires intermédiaires ». La directive a été transposée en France par la loi n° 2000-719 du 1er août 2000, modifiant la loi n° 86-1067 du 30 septembre 1986, relative à la liberté de communication dont les principales dispositions ont été modifiées par la loi n° 2004-575 du 21 juin 2004, pour la confiance dans l'économie numérique et le droit de la communication (dite LCEN).

Aujourd'hui, toute la difficulté est de déterminer avec certitude « qui fait quoi », autrement dit quelles sont les activités des différents acteurs d'Internet. Ainsi, lorsque la diffusion d'une information porte atteinte à la réputation d'un tiers, c'est au premier chef l'auteur de l'information lui-même qui devra en répondre. Toutefois, d'autres personnes, physiques ou morales, interviennent dans la chaîne de diffusion de l'information disponible sur Internet. Ce sont des fournisseurs, intermédiaires techniques, dont la responsabilité est parfois recherchée.

L'identification des fournisseurs Internet constitue un exercice d'autant plus délicat que leurs fonctions évoluent de façon constante. Il arrive même de plus en plus fréquemment qu'un même intermédiaire cumule plusieurs fonctions. Parmi les différents intermédiaires techniques, on distingue ainsi le fournisseur d'accès, le fournisseur d'hébergement et le transmetteur ou l'opérateur de télécommunications.

La principale fonction du fournisseur d'accès est « celle d'un prestataire de services de nature technique, chargé de mettre en relation ses abonnés avec les sites ou les autres utilisateurs »[182]. Il assure donc la connexion entre l'internaute et les sites. Le fournisseur d'hébergement « gère techniquement des ressources informatiques connectées à l'Internet et met ses ressources à disposition de l'abonné. Il accueille des sites d'éditeurs de contenu avec lesquels

[181] Aff. C-131-12, concl. Avocat général Niilo Jääskinen, §31.
[182] Conseil d'Etat, Internet et les réseaux numériques, Doc. fr., 2000, p. 186.

il est contractuellement lié, duplique des sites extérieurs, met en œuvre des services proxi et des serveurs news »[183]. Enfin, le transporteur ou opérateur de télécommunications est défini comme « toute personne physique ou morale exploitant un réseau de télécommunications ouvert au public et fournissant au public un service de télécommunications »[184]. Le terme désigne donc la personne qui, en vertu d'un contrat, assure le transport de l'information de l'ordinateur de l'utilisateur au serveur du fournisseur d'accès, puis du fournisseur d'accès aux ordinateurs des sites Internet ou des autres utilisateurs.

Ces notions font désormais l'objet d'une définition légale. Les fournisseurs d'accès, selon l'article 6, II, 1 de la LCEN, ont pour « activité d'offrir un accès à des services de télécommunication au public ». L'article 6, I, 2 définit, quant à lui, les hébergeurs comme : « Les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ».

La responsabilité de l'hébergeur peut, par conséquent, être engagée sur le fondement de la loi LCEN dans l'hypothèse où une personne est victime de la diffusion sur Internet d'un contenu illicite. Mais peut-on considérer que la législation actuelle qui organise cette responsabilité permet d'imposer aux intermédiaires techniques le respect d'un éventuel droit à l'oubli ? Plus encore, leur activité entre-t-elle dans le cadre de la protection des données personnelles ou doit-on aller plus loin et prévoir des règles spécifiques qui permettraient d'intégrer explicitement dans le champ de leurs obligations le respect d'un droit à l'oubli ?

Les textes ont certes encadré le statut des hébergeurs mais les techniques et les pratiques permises par Internet évoluent rapidement. En plus des hébergeurs, deux acteurs non envisagés par le législateur sont apparus sur la scène du Web 2.0[185] et leur traitement juridique demeure incertain. C'est le cas des fournisseurs de services de réseau social et des exploitants des moteurs de recherche. Nous aborderons donc successivement la situation des hébergeurs *stricto sensu*, des exploitants de moteurs de recherche et des fournisseurs de services de réseaux sociaux.

[183] Conseil d'Etat, Internet et les réseaux numériques, étude précitée, p. 185.
[184] L. n°96-659, 26 juill. 1996, art. 1er ; ainsi, par exemple, Orange ou Bouygues Telecom.
[185] Le Web 2.0, que désigne également comme le Web social, est le terme utilisé pour décrire l'ensemble des fonctionnalités et des techniques qui ont succédé à l'Internet dans sa forme initiale. Le Web 2.0 est plus simple et plus accessible. Il offre un réseau non plus statique, mais dynamique. L'internaute autrement dit, ne se borne plus à rechercher l'accès à une information, il peut également en créer, et en partager.

2.2.1. Les hébergeurs *stricto sensu*

Parmi les différents acteurs de la toile, les hébergeurs sont sans doute ceux dont le statut soulève le plus de questions dans la mesure où leur activité est difficile à délimiter. L'hébergeur est, nous l'avons indiqué, celui qui assure « *pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services* » (art. 6, I, 2 LCEN). Si l'on rapporte Internet à la problématique des données à caractère personnel, le droit à l'oubli pourrait être invoqué lors de la publication d'éléments et de données à caractère personnel sur des pages web d'Internet (dite page web source).

La qualification d'hébergeur est très convoitée en raison du statut particulièrement avantageux dont il bénéficie. La loi l'exonère, en effet, de toute responsabilité à condition qu'il n'ait pas connaissance de l'activité ou de l'information illicite ou, s'il en a connaissance, qu'il agisse rapidement pour retirer l'information litigieuse ou en supprimer l'accès[186].

Certains juges admettent qu'il puisse être amené à répondre de contenus illicites tant sur le fondement de la LCEN que de la loi informatique et liberté du 6 janvier 1978. On peut à ce sujet évoquer l'arrêt de la Cour d'appel de Montpellier en date du 15 décembre 2011[187]. En l'espèce un internaute ayant participé à un blog sous un pseudonyme se plaignait de ce qu'un tiers avait révélé, sur ce même blog, son identité de façon très précise ainsi que des éléments de sa vie privée. L'hébergeur à qui la victime avait demandé de supprimer ces informations ayant refusé d'y procéder, cette dernière agit en référé sur le double fondement de la loi de 2004 et de celle de 1978.

Pour que puisse être appliquée la loi de 1978, il faut pouvoir considérer que l'hébergeur est un responsable de traitement au sens de l'article 3. I. de la loi de 1978. Si tel est le cas, la victime pourrait s'opposer au traitement d'informations la concernant, en invoquant l'article 38 de la loi.

---

[186] Loi n° 2000/31/CE, 8 juin 2000, art. 14, et LCEN, art. 6, I, 2 : dont il résulte que « les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible ». L'alinéa 5 de ce même article ajoute que « la connaissance des faits litigieux est présumée acquise après notification notamment de la date, la description des faits litigieux et leur localisation précise, les motifs pour lesquels le contenu doit être retiré, comprenant la mention des dispositions légales et des justifications de faits ainsi que la copie de la correspondance adressée à l'auteur ou à l'éditeur des informations ou activités litigieuses demandant leur interruption, leur retrait ou leur modification, ou la justification de ce que l'auteur ou l'éditeur n'a pu être contacté ».

[187] A. Debet, L'hébergeur d'un blog est un responsable de traitement au sens de la loi Informatique et Libertés, Comm. com. électr., Avril 2012, comm. 41.

La définition du responsable de traitement englobe assurément l'éditeur du site ou du blog pour tout ce qui concerne le contenu de son blog. En revanche, si l'on s'en tient à la définition de la LCEN, l'hébergeur d'un blog apparaît avant toute chose comme un technicien. Il fournit les moyens techniques, un support numérique mais on peut douter de son implication dans les finalités du traitement qui correspondrait à l'objet d'un blog ou d'un site par exemple[188]. C'est *a priori* l'avis de la CNIL qui prévoit une dispense de déclaration pour les auteurs de blogs sans viser les hébergeurs[189].

De la même manière, la CNIL estime généralement que le prestataire qui fournit les moyens techniques d'un traitement (par exemple de la géolocalisation ou de la vidéosurveillance) n'est pas le responsable de traitement. En revanche, la personne qui utilise ces moyens, et l'on songe à l'employeur qui met en place ces techniques de surveillance au sein de l'entreprise, est qualifiée de responsable de traitement avec toutes les obligations légales qui découlent de ce statut.

Il est vrai que la position affichée par le G29 sur les réseaux sociaux[190] permet de s'interroger quant à la pertinence d'un tel raisonnement. Ce dernier considère en effet, nous y reviendrons, que les fournisseurs de services de réseaux sociaux (SRS) sont responsables du traitement des données : « ils fournissent les moyens permettant de traiter les données des utilisateurs ainsi que tous les services "basiques" liés à la gestion des utilisateurs (par exemple l'enregistrement et la suppression des comptes). Les fournisseurs de SRS déterminent également la manière dont les données des utilisateurs peuvent être utilisées à des fins publicitaires ou commerciales - y compris la publicité fournie par des tiers »[191]. Il convient alors de souligner qu'en pratique, entre un hébergeur de blog, proposant un certain nombre de services (comme le relevait la cour d'appel de Montpellier), et le fournisseur de services de réseaux sociaux tel que Facebook, la différence n'est pas toujours très nette notamment quand il s'agit d'examiner les contenus que des tiers laissent sur le blog ou sur la page d'un internaute, internaute qui fixe lui-même le thème de la discussion.

Dans l'arrêt précité du 15 décembre 2011, les juges ont considéré que « (…) la société JFG Networks, dans le cadre de la prestation qu'elle offre à ceux qui utilisent ses services de mise en ligne d'un blog, collecte les informations contenues dans les billets, les conserve tout en les organisant à la fois de façon ante-chronologique et de façon à les regrouper ou agglomérer au fil du temps sur un thème donné, tout en se réservant, ainsi que cela résulte de ses propres

[188] Le thème d'un forum de discussion sur un blog ou le type de produit ou services proposé sur un site, voir en ce sens A. Debet, préc..
[189] CNIL, délib. n° 2005-284, 22 nov. 2005 décidant la dispense de déclaration des sites web diffusant ou collectant des données à caractère personnel mis en œuvre par des particuliers dans le cadre d'une activité exclusivement personnelle (dispense n° 6).
[190] Avis 5/2009, 12 juin 2009 sur les réseaux sociaux en ligne.
[191] Avis 5/2009, préc., p. 5.

« Conditions générales d'utilisation », la faculté d'en suspendre la transmission ou diffusion, en cas d'abus de la part des utilisateurs »[192].

Par ailleurs, la société JFG Networks est amenée à traiter des données à caractère personnel dès lors que les informations ainsi stockées, organisées et diffusées, sont relatives à une personne physique parfaitement identifiée par ses nom, prénom et lieu de résidence. Dans ces conditions, dès lors que la loi de 1978 est applicable, le plaignant était fondé, à raison de l'atteinte à sa vie privée, à demander la suppression de son nom et prénom en vertu de son droit d'opposition sachant qu'il avait justifié s'être adressé à plusieurs reprises à la société JFG Networks en vue de cette suppression avant de l'assigner en référé.

La suppression du contenu peut également être obtenue sur le fondement de la LCEN. Dans cette même affaire, les juges se réfèrent à l'article 6, I, 8 de ladite loi qui énonce que « l'autorité judiciaire peut prescrire en référé ou sur requête, à toute personne mentionnée au 2 (les personnes physiques ou morale qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images de sons ou de messages de toute nature fournis par des destinataires de ces services) toute mesure propre à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne ». Or, dans la mesure où en l'espèce, l'atteinte à la vie privée est caractérisée au sens de l'article 9 du Code civil, les juges répondent favorablement à la demande de la victime d'enjoindre à l'hébergeur de faire cesser le dommage occasionné.

La qualification d'hébergeur offre donc à la victime de contenu ou de traitement illicites le droit d'obtenir le retrait du contenu litigieux mais nul besoin pour cela de consacrer un droit à l'oubli. On remarquera néanmoins que dans les deux cas évoqués, les informations diffusées portaient atteinte à la vie privée. Il serait intéressant de savoir dans quelle mesure la responsabilité de l'hébergeur pourrait être retenue en présence d'un contenu licite.

2.2.2. Les fournisseurs de services de réseaux sociaux

Internet est un lieu d'échange et de communication comme en témoigne le formidable essor des réseaux sociaux dont le succès augmente de jour en jour et touche, à des degrés variables il est vrai, toutes les couches et tous les âges de la population.

Les réseaux sociaux proposent des « services de réseautage social » (dits SRS) mais n'ont pas tous nécessairement la même finalité, ni les mêmes fonctionnalités. Certains réseaux

[192] Comm. com. électr., Avril 2012, comm. 41, A. Debet.

poursuivent une finalité sociale. C'est le cas de Facebook, MySpace ou Google+ par exemple. D'autres obéissent à une finalité bien spécifique tels LinkedIn ou Viadeo qui favorisent les réseaux professionnels. Dans certains cas, la finalité est encore plus précise. Ainsi en est-il d'un réseau comme Copainsdavant qui permet à ses membres de retrouver d'anciens camarades d'école ou d'activités sportives notamment.

Les SRS ont été définis par le G29 dans son avis du 5 juin 2009 sur les réseaux sociaux[193] comme « des plates-formes de communication en ligne permettant à des personnes de créer des réseaux d'utilisateurs partageant des intérêts communs ». Le G29 a recensé quatre caractéristiques communes à ces réseaux. En premier lieu, les utilisateurs, pour constituer leur « profil », sont invités à transmettre des données à caractère personnel. En deuxième lieu, les SRS proposent à leurs membres des outils destinés à mettre des contenus en ligne (des commentaires, de la musique, des photographies, des vidéos ou bien encore des liens vers d'autres sites, etc.)... En troisième lieu, les membres ont à leur disposition une liste de contacts avec lesquels ils ont la possibilité d'interagir. En quatrième et dernier lieu, dans la mesure où les informations fournies par les membres du réseau conduisent à élaborer un « profil » à partir duquel ils sont ciblés, les SRS trouvent là une source de financement de leur activité. En effet, les annonceurs peuvent ainsi cibler leur public et ce service se paye. Naturellement, plus la quantité d'informations données par les membres est importante, plus le ciblage est fin et plus les revenus publicitaires sont importants.

Il est évident, au vu de cette analyse, que les réseaux sociaux deviennent de proche en proche des mines d'informations parfaitement valorisables auprès des opérateurs économiques qui cherchent à mieux cibler leur public. En outre, ces réseaux constituant des espaces de communication entre les membres, ils accueillent et véhiculent des informations en tout genre.

Il convient dès lors de se demander quelle est la maîtrise des membres d'un réseau social sur les informations qu'ils transmettent. Les informations publiées sur les SRS sont en effet transmises volontairement par chaque membre. On peut donc considérer que l'internaute, membre d'un réseau social, est responsable des informations qu'il divulgue. D'ailleurs, les réseaux sociaux proposent tous des conditions générales d'utilisation qui doivent être lues et acceptées avant l'inscription[194]. Néanmoins, les activités des fournisseurs de SRS peuvent engendrer des situations préjudiciables pour ses membres ou pour les tiers et deux situations doivent être distinguées. D'une part, il est possible qu'un fournisseur de SRS véhicule des

[193] Voir l'avis du G29, WP 163, Avis 5/2009 sur les réseaux sociaux en ligne adopté le 5 juin 2009.
[194] Ces conditions sont régulièrement réactualisées. Le réseau social Facebook par exemple proposent de nouvelles conditions d'utilisation entrant en vigueur le 1er janvier 2015.

contenus concernant un de ses membres ou un tiers au réseau et peut alors se poser la question de la responsabilité de l'auteur du contenu. D'autre part, l'usage par des opérateurs économiques du contenu informationnel concernant un membre du réseau, sans être attentatoire à la vie privée d'un individu, peut lui être préjudiciable. L'on sait que des informations publiées par les utilisateurs peuvent être accessibles à des personnes non membres du réseau. Ainsi, nous l'avons indiqué, des cabinets de recrutement n'hésitent pas à consulter le profil des candidats, des employeurs s'enquièrent du profil de leurs salariés… On peut évoquer l'histoire de Stacy Snyder qui s'était vue reprocher d'avoir mis sur Internet une photo d'elle coiffée d'un chapeau de pirate et portant à sa bouche un gobelet en plastique, qu'elle avait elle-même intitulée « Pirate Ivre ». Considérant cette conduite « non-professionnelle », son université avait refusé de lui délivrer son diplôme. Lorsqu'elle voulut supprimer la photo du site Internet, la page avait déjà été cataloguée (ou capturée) et la photo archivée par des moteurs de recherche.

Dans cette hypothèse, le préjudice est réel (perte d'une chance) mais dans la mesure où la victime est l'auteur de la diffusion, aucune responsabilité ne peut en découler. Est-ce à dire que la diffusion fait disparaître toute possibilité de recours pour la victime et que l'information, une fois diffusée, ne serait donc plus maîtrisable. En dehors des systèmes numériques de mémoire, c'est une conséquence que l'on peut facilement admettre parce que son impact sera limité en principe. Un propos que l'on a tenu, une photo que l'on a laissé paraître dans un journal, une fois diffusés, ne sont plus maîtrisables. Mais le temps fait alors son effet. Une telle divulgation peut naturellement laisser des traces indélébiles sur la carrière de personnages publics, un politicien ou un acteur par exemple. En revanche, pour toute autre personne, le temps permet de retomber dans un certain anonymat, il permet l'effacement du souvenir grâce à l'oubli.

Avec Internet, la divulgation se traduit par une diffusion perpétuelle. Dès lors que la mémoire numérique ne permet plus à l'oubli de jouer naturellement son rôle, il devient pertinent de songer à la manière dont on pourrait imposer l'oubli dans ce cas de figure.

La loi informatique et libertés a déjà instauré, on l'a vu, un droit à l'effacement des données personnelles. La proposition de règlement européen relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données intitulait son article 17, « *Droit à l'oubli et à l'effacement* ». La résolution abandonne le droit à l'oubli pour ne retenir qu'un droit à l'effacement qui ouvre à chaque individu « le droit d'obtenir du responsable du traitement l'effacement de données à caractère personnel la concernant et la cessation de la diffusion de ces données (…) ». Le droit à l'oubli est réduit à un droit à l'effacement ce qui est en soi très discutable.

Sans viser directement les réseaux sociaux[195], les dispositifs actuels et à venir pourraient offrir une solution permettant de corriger les effets négatifs de la mémoire perpétuelle du numérique. Il convient donc de s'assurer de l'éligibilité des réseaux sociaux au dispositif de protection des données à caractère personnel avant d'envisager l'opposabilité d'un droit à l'oubli dans ce contexte spécifique.

2.2.2.1. L'éligibilité des réseaux sociaux au dispositif de protection des données à caractère personnel

Pour que les informations collectées sur les réseaux sociaux puissent accéder à un éventuel droit à l'oubli, il faut que soient réunies les conditions d'application de la loi Informatique et Libertés. L'application du dispositif est donc conditionnée par l'existence d'un traitement de données à caractère personnelle effectué par un responsable de traitement.

2.2.2.1.1. Un traitement de données à caractère personnel

Le *lifting* que les instances européennes se proposent d'opérer à la définition du traitement n'apporte rien de particulier s'agissant de la problématique des réseaux sociaux. En effet, tout d'abord, dans la mesure où les fournisseurs de SRS procèdent à l'enregistrement et à la conservation des informations fournies par les utilisateurs lors de l'inscription, mais également des informations publiées par les membres dans le cadre de leur activité sur le réseau, ils se livrent incontestablement à une activité de traitement de données. Les fournisseurs SRS peuvent également traiter les informations transmises par les membres du réseau aux fins de publicité ciblée. Ensuite, les fournisseurs d'application, en ce qu'ils utilisent les informations collectées sur les réseaux sociaux procèdent également au traitement de données. Enfin, les utilisateurs eux-mêmes, réalisent un traitement des données au titre de la diffusion d'information visée dans la loi de 1978 comme dans la proposition de règlement.

Le caractère personnel de ces données ne laisse pas davantage d'incertitudes dès lors qu'au moment même de son inscription sur le réseau, le futur membre est le plus souvent tenu de préciser son nom, son adresse mail, son âge ou encore son sexe par exemple. Il s'agit bien là de données propres à identifier une personne physique ce qui correspond à la définition de

[195] Les réseaux sociaux étaient plus nettement visés dans la proposition de 2012 dont le texte affirmait que ce droit concerne en particulier « des données à caractère personnel que la personne concernée avait rendues disponibles lorsqu'elle était enfant (…) » autrement dit, selon l'article 4 §18, lorsqu'elle était âgée de moins de 18 ans.

l'article 2 §2 de la loi du 6 janvier 1978 et *a fortiori*, à celle de l'article 4 §2 de la proposition amendée de règlement puisqu'elle ne fait que préciser la notion[196].

2.2.2.1.2. Un responsable de traitement

La multiplicité des acteurs intervenant sur les réseaux sociaux conduit à se demander qui peut être considéré comme responsable de traitement sur un réseau social. Le G29, dans son avis de 2009, a ainsi identifié trois responsables possibles : le fournisseur de SRS, le fournisseur d'applications et dans certains cas, l'utilisateur lui-même.

Les fournisseurs de SRS gèrent le réseau. Il s'agit très clairement d'organismes qui déterminent les finalités et les moyens du traitement. Les moyens sont « tous les services "basiques" liés à la gestion des utilisateurs » tels que « l'enregistrement et la suppression des comptes »[197]. Les finalités peuvent être l'utilisation des données des utilisateurs « à des fins publicitaires ou commerciales – y compris la publicité fournie par des tiers »[198]. Au regard tant des moyens que des finalités, les fournisseurs de SRS peuvent donc être considérés comme des responsables de traitement.

Les fournisseurs d'applications sont les opérateurs qui, en accord avec les fournisseurs de SRS, proposent aux utilisateurs des applications supplémentaires par rapport à celles proposées par le réseau social. Ces applications sont variées. Il s'agira de jeux en lignes, de comparateurs ou encore de services météo par exemple[199]. Les fournisseurs d'applications peuvent être amenés à traiter des données à caractère personnel des utilisateurs du réseau se servant de leurs applications. Dans ce cas, selon le G29, ils doivent eux aussi être considérés comme responsables de traitement.

Enfin, l'utilisateur du réseau s'inscrit volontairement sur un réseau social dans le but de partager des informations. Il en communique et il en reçoit puisque sa qualité de membre du réseau social lui offre un accès aux informations publiées par ses contacts et la possibilité de les utiliser (les conserver, les enregistrer, les diffuser notamment). D'un point de vue technique, on pourrait considérer qu'il traite lui-même des données puisque ses actes le conduisent à déterminer les finalités et les moyens du traitement.

---

[196] Rappelons que la disposition vise « toute information se rapportant à une personne physique identifiée ou identifiable (la "personne concernée"); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, par exemple à un nom, à un numéro d'identification, à des données de localisation, à un identifiant unique ou à un ou plusieurs éléments spécifiques, propres à l'identité physique, physiologique, génétique, psychique, économique, culturelle, sociale ou de genre de cette personne ».

[197] G29, avis n° 5/2009, p.5.

[198] *Ibid.*

[199] Pour une liste des applications sur le réseau social Facebook, voir par exemple le répertoire des applications disponible sur http://www.applications-facebook.org/repertoire_application.php.

Les réseaux sociaux peuvent d'ailleurs être un outil de recrutement, voire même de marketing[200] pour les autres utilisateurs. Ainsi en est-il d'un professionnel membre du réseau et traitant les données de ses contacts dans le cadre de son activité professionnelle, par exemple, pour se constituer un réseau ciblé. L'utilisateur d'un réseau supportera alors les mêmes obligations qu'un responsable de traitement[201] peu importe la finalité personnelle ou professionnelle du réseau.

Par conséquent, il ne fait aucun doute que les fournisseurs de SRS, les fournisseurs d'application mais également, les utilisateurs traitent des données à caractère personnel, que ce soit à des fins de gestion des comptes ou à des fins commerciales. L'examen des textes applicables et des projets démontre toutefois que l'application d'un droit à l'oubli numérique sur les réseaux sociaux risque de se heurter à de nombreux obstacles.

2.2.2.2. L'opposabilité d'un droit à l'oubli numérique dans le cadre des réseaux sociaux

En dépit d'une volonté politique forte de protéger les utilisateurs de réseaux sociaux, il n'est pas certain que la proclamation d'un droit à l'oubli permettrait de parvenir à son effectivité. Dans la proposition de règlement amendée (article 17 § 1), le droit à l'effacement des données ou des liens vers ces données ou de toute copie ou reproduction de celles-ci peut être invoqué lorsque, « a) les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées, b) la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe1, point a), ou lorsque le délai de conservation autorisé a expiré et qu'il n'existe pas d'autre motif légal au traitement des données; c) la personne concernée s'oppose au traitement des données à caractère personnel en vertu de l'article 19 c bis) un tribunal ou une autorité réglementaire basé(e) dans l'Union a jugé que les données concernées doivent être effacées et cette décision a acquis force de chose jugée ; d) les données ont fait l'objet d'un traitement illicite ». En réalité, la situation est bien plus complexe qu'il n'y paraît. En effet, lorsque les conditions de l'article 17 §1 sont remplies, le responsable du traitement et, le cas échéant, le tiers procède à l'effacement sans délai (article 17 §3). Néanmoins, le responsable de traitement est en droit de ne pas procéder à l'effacement

[200] V. E. Fraysse : *Facebook, Twitter et le web social, les nouvelles opportunités de business: stratégies, marketing, meilleures pratiques,* Agence Kawa, Numilog, 2e éd., 2011, 346 p. - Dans son discours sur l'Initiative « Futur de l'Internet » du Conseil Européen de Lisbonne (2 février 2009) : « l'Internet du futur: l'Europe doit jouer un rôle majeur », Viviane Reding, Membre de la Commission européenne responsable de la Société de l'Information et des Médias soulignait que l'on est passé du « Web 2.0 pour les loisirs » au « Web 2.0 pour la productivité et les services ».

[201] En ce sens, le G 29 affirmait que si l'utilisateur utilise le réseau « comme une plate-forme de collaboration pour une association ou une entreprise, (il) assume [...] l'entière responsabilité d'un responsable du traitement des données ».

lorsque la conservation des données à caractère personnel est nécessaire. L'appréciation de la nécessité de conserver des données n'est naturellement pas laissée à l'arbitrage du responsable de traitement, elle est encadrée. Pour autant force est de constater que l'opposabilité du droit à l'effacement sur les réseaux sociaux est largement obérée par un arsenal d'exceptions et semble en tout état de cause conditionnée par l'origine de la divulgation des données. En effet, l'une des particularités des données transmises dans le cadre des réseaux sociaux tient au fait qu'elles peuvent être de sources diverses, ce qui conduit à établir une différence de régime en fonction de l'origine de la diffusion des informations. Il est possible qu'elles émanent de la personne qu'elle concerne ou bien d'un autre utilisateur du réseau social.

2.2.2.2.1. Les données transmises par l'utilisateur

Les données transmises par l'utilisateur sont de deux sortes. Il y a d'une part, les données associées au compte et, d'autre part, les données diffusées dans le cadre de l'activité sur le réseau.

2.2.2.2.1.1. Les données d'identification associées au compte de l'utilisateur

Les données d'identification associées au compte de l'utilisateur qui sont transmises au fournisseur de SRS doivent pouvoir être invoquées au titre du droit à l'oubli numérique dans deux situations : lorsque l'utilisateur souhaite fermer son compte et lorsque les données d'identification changent. Il conviendra néanmoins, dans ce cas, de tenir compte des obligations légales de conservation.

L'article 6 §5 de la loi du 6 janvier 1978 impose une conservation des données « sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées ». La proposition amendée de règlement, dans son article 5 e) reprend une formule similaire mais précise, en outre, que « les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles ne seront traitées qu'à des fins de recherche historique, statistique ou scientifique ou pour être archivées conformément aux règles et aux conditions énoncées à l'article 83 et à l'article 83 bis et s'il est procédé à un examen périodique visant à évaluer la nécessité de poursuivre la conservation et, le cas échéant, que des mesures techniques et organisationnelles sont mises en place afin de limiter l'accès aux données à ces seules fins (minimisation de la durée de conservation) ». Plus encore, l'article 17 §3 d) de la proposition érige l'obligation légale de conservation des données à caractère personnel comme une exception directe au droit à l'effacement. Il prévoit en effet que la conservation des données

à caractère personnel est possible lorsqu'elle est nécessaire « au respect d'une obligation légale de conserver les données à caractère personnel prévue par le droit de l'Union ou par la législation d'un État membre à laquelle le responsable du traitement est soumis; la législation de l'État membre doit répondre à un objectif d'intérêt général, respecter le contenu essentiel du droit à la protection des données à caractère personnel et être proportionnée à l'objectif légitime poursuivi ».

S'agissant des réseaux sociaux, la difficulté portera sur la détermination du moment à compter duquel le traitement d'une donnée à caractère personnel cesse d'être nécessaire.

Dans une conception très stricte des dispositions législatives, le G29 a considéré que les données à caractère personnel associées au compte de l'utilisateur devraient être effacées lors de la suppression de son compte[202]. Cette proposition est toutefois immédiatement tempérée par une réserve selon laquelle les fournisseurs de services doivent conserver, à des fins légales et sécuritaires, pour une durée déterminée, des comptes et des données qui ont été mises à jour ou effacées afin d'empêcher les opérations malveillantes résultant de l'usurpation d'identité et d'autres délits. Cette réserve est suffisamment large pour constituer une brèche dans laquelle les fournisseurs ne manqueront pas de s'engouffrer afin de justifier la conservation de données.

Des exceptions légales de ce type existent déjà. La LCEN[203], complétée par un décret du 25 février 2011[204] impose aux hébergeurs et aux fournisseurs d'accès à Internet l'obligation de conserver pendant un an des données d'identification[205]. Si les fournisseurs de SRS peuvent être assimilés en tant qu'intermédiaires techniques à des hébergeurs, ils devront conserver « les identifiants de connexion ; l'identifiant attribué par le système d'information au contenu, objet de l'opération ; les types de protocoles utilisés pour la connexion au service et pour le transfert des contenus ; la nature de l'opération ; les date et heure de l'opération ; l'identifiant utilisé par l'auteur de l'opération lorsque celui-ci l'a fourni ».

Les fournisseurs de SRS ont également l'obligation[206], de conserver pendant un an à compter de la date de création du compte, « l'identifiant de (la) connexion ; les nom et prénom ou la raison sociale ; les adresses postales associées ; les pseudonymes utilisés ; les adresses de courrier électronique ou de compte associées ; les numéros de téléphone ; le mot de passe ainsi que les données permettant de le vérifier ou de le modifier, dans leur dernière version mise à jour ».

---

[202] G 29, Avis 5/2009, *op., cit*., p. 11.
[203] Article 2-2 de la LCEN
[204] Décret n° 2011-219 du 25 février 2011 *relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne*.
[205] Article 3 du décret.
[206] Article 1.3° du décret de 2011.

Au-delà de l'obligation légale de conservation, les fournisseurs de SRS peuvent souhaiter conserver des informations à des fins probatoires en prévision de litiges éventuels. Cette possibilité n'est pas prévue explicitement par les textes en vigueur mais entre dans les prévisions de l'article 17 §4 a) et b) de la proposition de règlement. « Au lieu de procéder à l'effacement, le responsable du traitement limite le traitement de données à caractère personnel de manière à ce qu'elles ne soient pas soumises aux manipulations usuelles d'accès aux données et de traitement des données exécutées par le responsable du traitement et qu'elles ne puissent plus être modifiées :

a) pendant une durée permettant au responsable du traitement de vérifier l'exactitude des données lorsque cette dernière est contestée par la personne concernée ;

b) lorsqu'elles ne sont plus utiles au responsable du traitement pour qu'il s'acquitte de sa mission, mais qu'elles doivent être conservées à des fins probatoires, Ainsi, le fournisseur SRS pourra conserver les données à caractère personnel pendant une durée permettant au responsable du traitement de vérifier l'exactitude des données lorsque cette dernière est contestée par la personne concernée mais aussi lorsqu'elles ne sont plus utiles au responsable du traitement pour qu'il s'acquitte de sa mission, mais qu'elles doivent être conservées à des fins probatoires ».

Il serait donc possible de conserver certaines informations jusqu'à l'extinction des délais de prescription des actions civiles ou pénales. En l'état du droit positif, on pourrait peut-être considérer que la conservation des données à caractère personnel le temps de l'extinction des délais de prescription correspond à une durée nécessaire au regard des finalités pour lesquelles elles sont traitées mais rien ne permet d'en être certain.

Il convient de préciser que faute de disposition légale prévoyant un délai de prescription, il ne s'impose pas en ce qui concerne les données de comptes inactifs ou abandonnés. L'inactivité d'un utilisateur n'est pas, en soi, une cause de suppression de ses données. La loi française et la directive européenne ne l'imposent pas. On pourrait imaginer que les réseaux sociaux se dotent de règles organisant le sort des comptes inactifs[207].

Plus spécifiquement, le décès du titulaire du compte n'entraîne pas automatiquement sa suppression, ni par conséquent, l'effacement des données[208]. Il faudrait en pareille situation que les ayants droit en fassent la demande. Mais même si la demande est formulée, l'obligation légale de conservation ne disparaît pas.

---

[207] Il s'agit d'ailleurs d'une des propositions du G29, Avis 5/2009, op., cit., p. 11 et proposition 14.

[208] Des estimations fondées sur la démographie des utilisateurs et sur le taux de mortalité permettent de dire qu'il y aurait 30 millions de comptes Facebook détenus par des personnes décédées, D. BUI, « L'éternité selon Facebook », Le nouvel observateur, 31 oct. 2013, n° 2556, p. 88.

2.2.2.2.1.2. Les données publiées sur le réseau

S'agissant des données publiées sur le réseau, *a priori*, ni le fournisseur de SRS, ni le fournisseur d'applications n'ont d'obligation légale de conservation. L'utilisateur peut donc, à leur égard, faire valoir un droit à l'oubli numérique des données qu'il a supprimées, droit qui se matérialisera par un effacement des données. La proposition de règlement reprend le principe du consentement de la personne concernée au traitement de ses données[209] mais ajoute au dispositif en introduisant son corollaire, le droit de retirer son consentement. L'article 6 §1 a) énonce en effet que le traitement de données à caractère personnel n'est licite qu'à certaines conditions, notamment, que la personne concernée ait « consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ». L'article 7 §3 prévoit, corrélativement, le droit pour la personne concernée « de retirer son consentement à tout moment » étant précisé que « le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement préalablement donné » mais ouvre droit, nous l'avons souligné plus haut, à l'effacement des données (article 17 §1 b). Sans cibler spécifiquement les réseaux sociaux, le texte pourrait bien répondre à leur problématique. On pourrait concevoir que toute donnée supprimée par l'utilisateur voire même, tout compte supprimé, correspondraient à un retrait du consentement de la personne au traitement de ses données. Le champ d'application du droit à l'effacement des données serait alors extrêmement large puisqu'il en résulterait que toute suppression de données par l'utilisateur entraînerait un effacement immédiat et définitif par le fournisseur de SRS. Néanmoins, dans ce cas de figure, on peut penser que des motifs sécuritaires pourraient justifier leur conversation.

Ajoutons que les réseaux sociaux sont le terrain idéal pour le recueil de données qui, au sens des législations européenne et française, sont qualifiées de « sensibles ». Les utilisateurs de réseaux sociaux peuvent ainsi livrer directement ou indirectement des informations touchant leur santé, leur orientation sexuelle, leurs opinions politique ou religieuse. De façon directe, ils peuvent être amenés à renseigner leur « statut de profil » ou à laisser des « commentaires ». De façon indirecte, la fonction « j'aime » ou « *like* » utilisée au sujet d'informations publiées par un membre peut être particulièrement intrusive sans que l'utilisateur en ait nécessairement conscience. Les données, si elles sont traitées, tombent alors sous le coup de l'article 8 §1 de la

[209] La loi du 6 janvier 1978 (article 7) a généralisé le principe du consentement préalable lors de la révision opérée en 2004. Compte tenu de la rigidité d'une telle condition, la loi prévoit néanmoins des exceptions à son recueil. Ainsi, le consentement préalable de la personne n'est pas requis lorsque le traitement tend à la « réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée » (article 7§5).

loi de 1978 qui prévoit qu'il « est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci »[210] texte repris par les propositions en cours.

La suppression des données s'appliquera également aux données concernant des personnes décédées. Le décès ne paraît pas, en effet, justifier un traitement différent. Facebook a néanmoins mis en place un dispositif spécifique applicable dans cette hypothèse en proposant un formulaire décès qui permet soit de désactiver le compte, soit de mettre la page en mode mémoriel[211]. Il s'agit d'une page permettant d'accueillir des commentaires mais elle est configurée pour éviter les maladresses du dispositif de relance de Facebook du type « *Connaissez-vous cette personne ? Invitez-la à devenir votre amie !* ». Naturellement, il s'agit là d'une possibilité pour les ayants droit et non d'une obligation et l'on constate que les proches d'une personne décédée souhaitent parfois maintenir l'activité du compte afin d'éviter que la personne ne tombe définitivement dans « l'oubli »[212].

Des mesures préventives permettent en théorie de limiter les conséquences préjudiciables de l'activité menée sur les réseaux sociaux. Ainsi, certains fournisseurs limitent toute inscription de membres n'ayant pas atteint un âge minimal qu'ils définissent. L'article 8 de la proposition de règlement prévoit d'ailleurs un régime spécifique de traitement pour les données concernant des enfants de moins de 13 ans. Le traitement n'est licite « que si et dans la mesure où le consentement est donné ou autorisé par un parent de l'enfant ou par son tuteur légal »[213]. On peut raisonnablement s'interroger sur l'efficience de telles mesures. En pratique, il apparaît d'une part, que les conditions générales d'utilisation manquent parfois de clarté et, d'autre part, que les limites d'âge prévues sont facilement contournables et sont très fréquemment contournées[214]. Néanmoins, on ne peut nier qu'il s'agit de précautions minimums indispensables qui ont nécessairement un impact sur une éventuelle responsabilité de ces réseaux. Les instances européennes ont bien conscience de ces limites pratiques et la proposition de règlement limite considérablement le poids de la responsabilité des responsables

[210] Article 8 §1 de la directive 95/46.
[211] Politique de confidentialité Facebook, partie « Compte de commémoration ».
[212] D. Bui, « L'éternité selon Facebook », préc..
[213] Article 8§1 de la résolution.
[214] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:FR:PDF. Voir l'étude réalisée en 2011 par TNS SOFFRES pour la CNIL qui révèle que près de 20% des moins de 13 ans ont un compte et que 48% des enfants de 8 à 17 ans sont connectés à un réseau social, tout particulièrement, Facebook.

de traitement en précisant à l'article 8 §1 que « le responsable du traitement s'efforce raisonnablement de vérifier le consentement, compte tenu des moyens techniques disponibles, sans pour autant entraîner de traitement inutile de données à caractère personnel ». Il s'agit donc d'une obligation de moyens et, en aucun cas, de résultat[215]. En pratique, concernant la sécurité des mineurs, Facebook encourage les parents à expliquer à leurs enfants les pratiques de sécurité sur Internet[216]. De plus, il peut mettre en place des contrôles spéciaux (mise en place de restrictions sur la capacité des adultes à partager des informations et à prendre contact avec eux annoncé depuis le 16 octobre 2013), de telles mesures pouvant restreindre l'expérience des personnes mineures sur Facebook. Par ailleurs, il enseigne aux mineurs les implications des publications publiques, par l'instauration d'une étape dite de « pédagogie avancée », protège également les informations sensibles, comme par exemple les coordonnées, écoles et date de naissance des mineurs en faisant en sorte qu'elles n'apparaissent pas dans une recherche publique. De même, il rappelle aux mineurs qu'ils devraient uniquement accepter les demandes d'ajout à la liste d'amis des gens qu'ils connaissent. Enfin, le réseau social a instauré une protection supplémentaire sur les messages des mineurs. Cette protection empêche les mineurs de recevoir des messages d'inconnus tout en leur permettant de recevoir les messages de leurs amis, des amis de leurs amis et d'autres personnes qu'ils pourraient connaître. Facebook interdit toutefois aux mineurs de s'inscrire au réseau s'ils ont moins de 13 ans[217].

2.2.2.2.2. Les données divulguées par un utilisateur tiers

Les données divulguées par un utilisateur tiers peuvent concerner un autre membre du réseau ou une personne extérieure au réseau. Dans ces deux cas, le régime juridique applicable sera le même. L'étude de la jurisprudence sur la relation de faits ou d'événements par une personne tierce met en exergue la difficulté à consacrer le droit à l'oubli et rien ne justifie que le traitement juridique de ces situations diffère lorsque le support de la diffusion est numérique. Un principe fondamental et de portée générale s'y oppose, celui de la liberté d'expression.

Cette liberté n'est cependant pas sans limite et une distinction doit être faite selon le caractère du contenu. Si le contenu de l'information divulguée est *illicite* (diffamatoire, injurieux ou portant atteinte à la vie privée), la victime peut en demander le retrait au fournisseur

[215] Le paragraphe 1 bis ajoute : « Les informations fournies aux enfants, aux parents et aux tuteurs légaux, y compris en ce qui concerne la collecte et l'utilisation des données par le responsable du traitement, devraient être communiquées dans des termes clairs adaptés au public visé ».
[216] Politique de confidentialité Facebook, partie « Personnes mineurs et sécurité ».
[217] http://www.lemonde.fr/technologies/article/2013/10/17/facebook-limite-l-acces-aux-publications-des-mineurs_3496972_651865.html

de SRS sur la base des dispositions de la LCEN du 6 août 2004 ou de la loi Hadopi II. Néanmoins, l'auteur du propos pourrait être tenté d'invoquer le caractère privé de la diffusion dès lors qu'il l'a limitée à un cercle restreint de personnes. La jurisprudence a néanmoins tranché la question en droit du travail. Le conseil des prud'hommes a en effet tiré les conséquences du comportement de deux salariées ayant tenu sur le réseau social Facebook des propos dénigrants et incitant à la rébellion à l'égard de leur supérieure hiérarchique nommément désignée, en validant leur licenciement. L'abus de la liberté d'expression a été reconnu compte tenu, notamment, des fonctions qu'elles exerçaient (chargées de recrutement en contact avec des candidats et futurs salariés) mais également, et c'est ce point qui est intéressant, des paramètres de confidentialité choisis : leur « profil » étant accessible à leurs « amis Facebook » et aux « amis de leurs amis », les propos tenus ont été considérés comme publics[218]. Les conditions d'utilisation d'un réseau social peuvent donc faire tomber les propos qui y sont tenus dans la sphère publique et interdire en conséquence d'invoquer la violation du droit au respect de la vie privée contre les employeurs qui viendraient à se prévaloir de ces propos. S'agissant du mur Facebook, « il s'apparente à un forum de discussion qui peut être limité à certaines personnes ou non » et « en y postant un message, le salarié s'expose à ce que tout individu inscrit sur Facebook puisse accéder librement à ces informations (coordonnées, mur, messages, photos) »[219].

A l'inverse, la divulgation d'un contenu *licite* par un utilisateur tiers ne saurait justifier un retrait sous peine d'attenter à la liberté d'expression. C'est bien à cette situation que correspond l'article 17 §3 a) de la proposition de règlement qui prévoit que la conservation des données à caractère personnel est possible lorsqu'elle est nécessaire «à l'exercice du droit à la liberté d'expression, conformément à l'article 80 ».

En outre, il a été indiqué plus haut que l'utilisateur d'un réseau social était lui-même un responsable de traitement. Il devrait à cet égard supporter la même responsabilité. Néanmoins, ce serait faire fi d'une exception essentielle. En effet, si le traitement intervient « pour l'exercice d'activités exclusivement personnelles »[220], le responsable n'est pas soumis aux exigences légales mais bénéficie de « l'exemption domestique ». La proposition de règlement reprend cette exception et exclut également du champ d'application du règlement les activités de traitement réalisées « par une personne physique sans but lucratif dans le cadre de ses activités

[218] Cons. prud'h Boulogne-Billancourt., 19 novembre 2010, n°09/00316 et n°09/00343, RJS 01/11, n°5, p25. Voir également : TGI Béthune., 14 décembre 2010, Sté Access from Everywhere c/ E.N : www.legalis.net.
[219] CA Reims., 9 juin 2010, RJS 01/11, n°5, p25. CA Besançon., 15 novembre 2011, n°10/02642, SSS 21 janvier 2013, n°1568, p12. Voir cependant : CA Rouen., 15 novembre 2011, n°11/01380, Jurisprudence Sociale Lamy, 9 février 2012, n°315, p27.
[220] Article 2 §1 de la loi du 6 janvier 1978.

exclusivement personnelles ou domestiques » (article 2 §2 d) les parlementaires ayant proposé d'ajouter que « Cette dérogation s'applique également à une publication de données à caractère personnel lorsqu'il peut raisonnablement être escompté que seul un nombre limité de personnes y aura accès ». Il y a là, nous semble-t-il, une référence aux réseaux sociaux sur lesquels il est possible de limiter le nombre de personnes à qui l'on souhaite diffuser une information.

Lorsque l'utilisateur d'un réseau social traite des données à caractère personnel, dans la majorité des cas, la « finalité du traitement » est purement personnelle. C'est le cas de Facebook ou de Copainsd'avant par exemple. Il jouit dans ce cas de « l'exemption domestique ».

En conclusion, il apparaît que les réseaux sociaux sont une mine de données à caractère personnel ce qui n'est pas sans danger pour les utilisateurs. Diverses dispositions légales offrent aux personnes concernées des garanties minimales destinées à limiter les atteintes et les opérateurs mettent en œuvre des mesures préventives dans le but de sensibiliser les personnes les plus vulnérables. Il est bien évident qu'un droit de contrôle absolu par l'utilisateur n'est pas envisageable car les réseaux sociaux constituent un vecteur d'information en tout genre qui peut être détourné de sa finalité première pour abriter des activités sensibles voire condamnables (incitation au terrorisme notamment). Le choix de la personne de diffuser des informations la concernant l'engage et la rend débitrice d'un certain nombre d'obligations dans l'intérêt général.

Cette remarque permet de mieux identifier l'objectif qui pourrait être alloué à un droit à l'oubli, et ce faisant, conduit à définir son champ d'application et ses limites. Au fond, on doit permettre la conservation des données lorsqu'un intérêt supérieur le requiert mais cette considération n'empêche pas d'admettre que des limitations au traitement pourraient être apportées : ainsi, un droit à l'oubli justifierait qu'une personne puisse s'opposer à la diffusion d'une information la concernant mais pas à la conservation d'une information dès lors que les conditions légales l'exigeant sont remplies. Toute la difficulté néanmoins tient à ce que les utilisateurs ne disposent d'aucun moyen technique de vérifier quelles sont les informations qui sont conservées[221].

2.2.3. Les moteurs de recherche

Les moteurs de recherche, dans leur rôle d'indexation des pages web source, ont-ils une responsabilité à l'égard des personnes visées dans certaines de ces pages ? Peuvent-ils être tenus de procéder à la désindexation d'une page web ? Sur quel fondement ?

[221] Voir *infra* l'analyse technique sur ce point.

Au regard de la protection des données à caractère personnel et d'un éventuel droit à l'oubli, deux activités exercées par les fournisseurs de services de moteur de recherche peuvent être répertoriées. La première réside dans la fourniture par un moteur de recherche des résultats de recherche qui dirigent l'utilisateur Internet vers la page web source. La seconde activité, sans doute la moins visible pour l'utilisateur, consiste pour le moteur de recherche, à récupérer certaines données à caractère personnel de l'internaute qui se livre à une recherche sur Internet, telles que l'adresse IP à partir de laquelle la recherche est effectuée. Les informations auxquelles on accède en utilisant les services de recherche peuvent être de nature juridique différente. Le traitement judiciaire des demandes tendant à opposer aux fournisseurs de moteurs de recherche un droit à l'oubli est actuellement réglé de deux manières. Les juges considèrent que l'information en question constitue soit une donnée à caractère personnel faisant l'objet d'un traitement illicite, soit un contenu illicite pouvant être sanctionné sur un fondement spécifique, généralement le droit au respect de la vie privée (la même information pouvant avoir ces deux caractères).

2.2.3.1. La responsabilité du moteur de recherche pour traitement illicite d'une donnée à caractère personnel

Si le contenu auquel renvoie le moteur de recherche constitue une donnée à caractère personnel, la personne concernée pourra en limiter la diffusion à condition d'établir que ces données font l'objet d'un traitement illicite par un responsable de traitement qui doit être sanctionné sur la base de la loi informatique et libertés. Si la qualité de responsable de traitement, indispensable à la mise en jeu de la responsabilité du fournisseur de services de moteur de recherche, a pu un temps être mise en doute, le rôle amplificateur qu'il joue dans la recherche d'informations a fini par convaincre de cette qualité.

2.2.3.1.1. La qualité discutée de responsable de traitement

Même si la définition du responsable de traitement est large, on l'a vu, il n'était pas certain qu'elle couvre les fournisseurs de moteur de recherche. La Cour de Justice de l'Union Européenne a été saisie de cette question dans l'affaire C-131/12 Google Spain c/ AEPD[222]. En l'espèce, un citoyen espagnol avait demandé en 2009 au journal *La Vanguardia* la suppression

[222] Décision du 13 mai 2014, JCP G 2014, p. 768, note L. Marino ; JCP E 2014, p. 1327, note G. Busseuil ; JCP E 2014, p. 1326, note M. Griguer. – V. aussi, Conseil d'Etat, « Le numérique et les droit fondamentaux », Les rapports du Conseil d'Etat, sept. 2014, p. 187 et suiv..

d'une publication concernant une saisie de biens résultant du non-paiement de dettes contractées mais finalement remboursées auprès de la sécurité sociale espagnole plusieurs années auparavant. Au cours de la procédure administrative devant l'Agencia Española de Protección de Datos (AEPD), le journal n'a pas pu accéder à la demande de M. X, l'information faisant l'objet d'une publication légale ordonnée par le Ministère du Travail et des Affaires Sociales espagnol. C'est la raison pour laquelle M. X a décidé d'agir contre Google Inc et Google Spain S.L. afin qu'ils mettent en place « les mesures nécessaires pour obtenir le retrait et rendre impossible l'accès futur à ces données ». L'AEPD lui ayant donné raison, Google Inc et Google Spain S.L. ont formé un appel devant *l'Audiencia Nacional* et sollicité la nullité de la résolution administrative. Cette dernière a décidé de surseoir à statuer pour poser à la CJUE une série de questions préjudicielles touchant à la notion de droit à l'oubli, à l'application territoriale de celui-ci et enfin à la responsabilité des moteurs de recherche en matière de protection des données à caractère personnel.

Le raisonnement qui avait été préconisé par l'avocat général reposait sur l'application d'un principe de proportionnalité que l'on peut qualifier d'approche coût-bénéfice. Il soulignait l'importance du rôle joué par les moteurs de recherche dans la société de l'information et considérait que : « L'accessibilité universelle des informations sur l'Internet dépend en réalité des moteurs de recherche, puisqu'il serait trop compliqué et difficile de trouver sans eux les informations pertinentes, et l'on n'obtiendrait que des résultats limités. (…), il aurait fallu autrefois se rendre aux archives du journal pour obtenir des informations sur les annonces concernant la vente forcée de la propriété de la personne concernée. Aujourd'hui, ces informations peuvent être obtenues en entrant le nom de cette personne dans un moteur de recherche sur Internet, ce qui accroît considérablement l'efficacité de la diffusion de telles informations, tout en la rendant plus perturbante pour la personne concernée. Les moteurs de recherche sur Internet peuvent être utilisés pour établir un profil exhaustif des individus par la recherche et la collecte de leurs données à caractère personnel. Or ce sont précisément les craintes relatives à l'établissement de tels profils qui ont été à l'origine du développement de la législation moderne en matière de protection des données à caractère personnel »[223].

Il est aisé d'admettre qu'un prestataire de moteur de recherche opère un traitement de données à caractère personnel. Néanmoins, au regard de l'interprétation jurisprudentielle de l'article 2 d) de la directive de 1995, ce prestataire semble rentrer difficilement dans l'habit d'un *responsable* de traitement qui est « la personne physique ou morale (…) qui détermine les finalités et les moyens du traitement de données à caractère personnel ». En effet, lorsque la

[223] Aff. C-131/12, concl. Avocat général Niilo Jääskinen, §45.

directive de 1995 a été adoptée, Internet en était à ses balbutiements sans que l'on puisse alors imaginer l'explosion qui a suivi et toutes les applications qui en ont été réalisées par la suite. Impossible donc pour ses rédacteurs d'imaginer que des informations éditées sur un site Internet puissent être copiées, séquencées et diffusées par des personnes totalement étrangères à l'éditeur ou à l'hébergeur. Il est vrai que d'un point de vue strictement littéral, un moteur de recherche détermine les moyens et les finalités du traitement de données à caractère personnel. Néanmoins, pour l'avocat général, le *responsable du traitement* est celui qui est « conscient de l'existence d'une certaine catégorie définie d'informations correspondant à des données à caractère personnel, et (qui) les traite en étant animé de quelque intention en rapport avec leur traitement *en tant que* données à caractère personnel »[224]. Cette approche est aussi celle du G29 pour qui la « notion de responsable du traitement est une notion fonctionnelle, visant à attribuer les responsabilités aux personnes qui exercent une influence de fait (…), elle s'appuie donc sur une analyse factuelle plutôt que formelle »[225]. Le traitement d'un simple code informatique, aurait-il pour conséquence de conduire au traitement d'une donnée à caractère personnel, ne serait donc pas susceptible d'engendrer cette responsabilité. L'approche privilégiée par le G29 est d'ailleurs à rapprocher de celle qui a été consacrée par la CJUE dans le contentieux relatif aux places de marché en ligne notamment. En effet, dans l'un comme dans l'autre cas, la responsabilité serait conditionnée par le rôle actif de l'intermédiaire[226] autrement dit par le fait qu'il exerce un « contrôle réel sur les données à caractère personnel traitées »[227].

Par conséquent, pour l'avocat général, « si les fournisseurs de services de moteur de recherche sur Internet étaient considérés comme des responsables du traitement de données à caractère personnel sur des pages web source de tiers et que figuraient sur ces pages des «catégories particulières de données», telles que visées à l'article 8 de la directive (c'est-à-dire des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que des données relatives à la santé et à la vie sexuelle), l'activité du fournisseur de services de moteur de recherche sur Internet deviendrait automatiquement illégale, dès lors que les conditions strictes prévues dans cet article pour le traitement de telles données ne seraient pas remplies »[228].

[224] Aff. C-131/12, concl. Avocat général Niilo Jääskinen, §82.
[225] Groupe de travail «Article 29», avis 1/2010, p. 10.
[226] Groupe de travail «Article 29», avis 1/2008, p. 15.
[227] Aff. C-131/12, concl. Avocat général Niilo Jääskinen, §85.
[228] Aff. C-131/12, concl. Avocat général Niilo Jääskinen, § 90.

Si l'on adoptait cette conception, devrait-on alors considérer que ces opérateurs sont à l'abri de toute responsabilité ? Non, assurément pas. Ainsi, même si le cache résulte de processus entièrement techniques et automatisés, les contenus de la mémoire cache des moteurs de recherche pourraient faire de ces opérateurs des responsables de traitement dès lors qu'ils ne respectent pas les codes d'exclusion imposés par les éditeurs de sites Internet ou s'ils ne mettaient pas à jour une page web dans la mémoire cache, en dépit d'une demande en ce sens de l'éditeur du site car dans ces deux hypothèses, le contenu des informations relève bien du contrôle du fournisseur de services[229]. De même, dans certaines hypothèses, le moteur de recherche prend lui-même l'initiative de recueillir, croiser et utiliser des données, des traces, disséminées dans différents « sites » ou « outils » qu'il gère directement. C'est le cas du moteur de recherche Google lorsqu'il associe des données recueillies lors de l'utilisation de différentes ressources qu'il propose aux internautes. Ceci qu'ils soient authentifiés, comme c'est le cas avec Google mail, ou pas, par exemple en se référant à d'autres traces laissées lors des passages et leur association avec des informations identifiantes comme l'adresse IP ou avec les sites visités, ce qui permet de profiler les internautes. Dans ce contexte, se pose la question de la légitimité du traitement des données à caractère personnel auquel la personne concernée n'aura pas donné son consentement. Il y a tout lieu de penser que c'est l'intérêt légitime du traitement, au sens de l'article 7 f) de la directive de 1995, qui permettra de s'en dispenser. En effet, l'activité des moteurs de recherche poursuit incontestablement un intérêt légitime dans la mesure où elle facilite l'accès des informations aux internautes et contribue à une meilleure diffusion des informations mises en ligne. L'avocat général faisait également référence à l'offre de services de la société de l'information, accessoires au moteur de recherche, tels que l'offre de publicité par mots clés. Trois finalités qui, selon ce dernier, « se rapportent respectivement à trois droits fondamentaux garantis par la Charte, à savoir la liberté d'information et la liberté d'expression (toutes deux consacrées à l'article 11) et la liberté d'entreprise (article 16) »[230].

Naturellement, dans ce cas de figure, les exigences énoncées à l'article 6 de la directive s'imposent au moteur de recherche qui doit s'assurer que les données à caractère personnel sont « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement »[231] mais également « exactes et, si nécessaire, mises à jour; toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées »[232].

[229] Aff. C-131/12, concl. Avocat général Niilo Jääskinen, § 93.
[230] Aff. C-131/12, concl. Avocat général Niilo Jääskinen, § 95.
[231] Article 6 c).
[232] Article 6 d).

Pour l'avocat général, il convient que les intérêts du «responsable du traitement, ou des tiers dans l'intérêt desquels le traitement est effectué, ainsi que ceux de la personne concernée », soient mis en balance en vue d'une pondération[233].

2.2.3.1.2. Une responsabilité liée au rôle amplificateur du moteur de recherche

Bien avant que ne soit saisie la CJUE, des juges français s'étaient placés sur le terrain de la loi de 1978 pour sanctionner les fournisseurs de moteurs de recherche. Dans une ordonnance de référé du 28 octobre 2010, le TGI de Montpellier[234] a statué sur une demande de déréférencement vers un site proposant une vidéo pornographique, demande faite par une femme qui, devenue enseignante, se plaignait du trouble que lui causait le renvoi automatique à ces pages lorsque l'on tapait son nom dans le moteur de recherche Google. Le Tribunal a retenu l'existence d'un trouble manifestement illicite découlant à la fois d'une atteinte à la vie privée et d'un traitement illicite de données à caractère personnel. Concernant le traitement illicite de données à caractère personnel, le juge des référés considère que l'indexation des pages *web* et leur mise à la disposition des internautes réalise un traitement de données à caractère personnel. La loi du 6 janvier 1978 a donc vocation à s'appliquer. Pour le juge en effet, le moteur de recherche devait « aménager la possibilité d'un retrait *a posteriori* des données à caractère personnel en permettant la désindexation des pages à la demande de la personne concernée par ces données en application de l'article 38, alinéa 1er » de la loi du 6 janvier 1978 qui offre un droit d'opposition à la personne dont des données personnelles ont été traitées. On peut se demander si c'était la disposition la plus pertinente en l'espèce car la demande conduit plutôt, dans cette hypothèse, à une rectification prévue par l'article 40, alinéa 1er[235]. Plus précisément, pour le juge des référés, ce n'est pas le traitement par le moteur de recherche des données à caractère personnel de la victime qui est illicite, mais bien l'inaction de celui-ci, à compter de la demande de désindexer les pages *web* litigieuses, qui constitue un trouble manifestement illicite.

Cette solution est jugée insatisfaisante pour une partie de la doctrine qui estime que, « à supposer que la société Google Inc. procède bien au déréférencement de tous les résultats précités, cela ne fera pas disparaître la vidéo de la toile, où elle continuera d'être librement accessible, par exemple par le truchement d'un autre moteur ou bien, directement, à partir de la

[233] Aff. C-131/12, concl. Avocat général Niilo Jääskinen, § 96.
[234] TGI Montpellier, ord. Réf, 28 oct. 2010, Comm. com. électr. n°5, Mai 2011, comm. 47, A. Lepage.
[235] Article qui énonce, nous l'avons vu : « toute personne physique justifiant de son identité » d' « exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite ».

connaissance des URL ». Sans doute, mais cela ne justifie pas véritablement une mise à l'écart de la loi de 1978. Compte tenu des millions de sites abrités sur la toile, les moteurs de recherche sont en effet devenus des outils incontournables de la recherche sur Internet. L'effacement définitif d'un contenu ne peut techniquement être garanti et n'est pas toujours justifié d'ailleurs. Dès lors, limiter les voies d'accès à un contenu semble une alternative tout à fait intéressante à condition de l'encadrer strictement.

Précisément, cette position a été consacrée par la Cour de justice de l'Union européenne dans l'affaire Google Spain c/ AEPD par la décision du 13 mai 2014 dont le premier point pose en principe que les moteurs de recherche, en raison de leur activité de traitement spécifique, peuvent être assimilés à des responsables de traitement. Elle énonce d'une part, que « l'activité d'un moteur de recherche consistant à trouver des informations publiées ou placées sur Internet par des tiers, à les indexer de manière automatique, à les stocker temporairement et, enfin, à les mettre à la disposition des internautes selon un ordre de préférence donné doit être qualifiée de *traitement de données à caractère personnel*, au sens de cet article 2, sous b), lorsque ces informations contiennent des données à caractère personnel » et, d'autre part, que « l'exploitant de ce moteur de recherche doit être considéré comme le *responsable* dudit traitement, au sens dudit article 2, sous d) » parce que son activité de traitement se distingue et s'ajoute à celle des éditeurs de sites qui font figurer des données sur des pages Internet[236]. Il est bien évident que l'activité de traitement des moteurs de recherche joue un rôle déterminant dans la diffusion globale des données personnelles puisqu'il permet à tout internaute d'accéder à ces données en effectuant une recherche à partir du nom d'une personne « y compris aux internautes qui, autrement, n'auraient pas trouvé la page web sur laquelle ces mêmes données sont publiées »[237]. Il en résulte que l'activité d'un moteur de recherche peut affecter significativement et de manière additionnelle par rapport à celle des éditeurs de sites web les droits fondamentaux de la vie privée et de la protection des données à caractère personnel[238].

La décision nous fait toucher du doigt un droit à l'oubli numérique mais on remarquera qu'à aucun moment la Cour de justice ne fait de référence explicité au terme « droit à l'oubli ». La décision démontre, point par point, que le dispositif de protection des données à caractère personnel suffit en lui-même à protéger la personne concernée.

La décision va dans le sens de la nouvelle version de l'article 17 §1 de la proposition de règlement qui étend explicitement le droit à l'effacement à tous les liens vers des données à

[236] Sur ce tout dernier point, voir les §35 et suiv. de la décision.
[237] CJUE, aff. C-131/12, §36.
[238] CJUE, aff. C-131/12, §38. Voir aussi, CNIL, Droit au déréférencement Interprétation commune de l'arrêt de la CJUE http://www.cnil.fr/fileadmin/documents/Vos_libertes/Droit_au_dereferencement-Interpretation-Arret.pdf

caractère personnel concernant l'intéressé, ce qui se traduit par un droit à la désindexation ou au déréférencement. Cette décision n'a pas manqué de soulever des critiques de la part de l'intéressé naturellement, mais également d'autres acteurs économiques tels que les journalistes (à travers Reporters sans frontières) ou La quadrature du net. Il faut toutefois convenir que, en pareille hypothèse, seul est en cause le rôle amplificateur du moteur de recherche dans la diffusion d'une information qui n'est plus d'actualité. Ni plus, ni moins. Or, nous l'avons souligné, tout l'intérêt de cette décision est précisément d'offrir aux victimes de la diffusion d'un contenu licite mais dépassé un moyen de faire oublier au grand public cet événement de leur vie sans toutefois tronquer la réalité. La Cour de justice précise d'ailleurs que : « Les articles 12, sous b), et 14, premier alinéa, sous a), de la directive 95/46 doivent être interprétés en ce sens que, afin de respecter les droits prévus à ces dispositions et pour autant que les conditions prévues par celles-ci sont effectivement satisfaites, l'exploitant d'un moteur de recherche est obligé de supprimer de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, des liens vers des pages web, publiées par des tiers et contenant des informations relatives à cette personne, également dans l'hypothèse où ce nom ou ces informations ne sont pas effacés préalablement ou simultanément de ces pages web, et ce, le cas échéant, même lorsque leur publication en elle-même sur lesdites pages est licite ». Il s'agit donc bien de limiter la diffusion des résultats sans remettre en cause l'existence même du contenu qui demeure licite. En revanche, il est vrai que la solution n'est pas sans faille puisqu'elle ne vise qu'un moteur de recherche dont certains internautes pourraient finir par se détourner[239].

Le 30 mai 2014, la société Google a pris acte de la décision de la CJUE en annonçant, contre toute attente, qu'elle mettait à disposition des internautes un formulaire destiné à permettre une désindexation. Il s'agit néanmoins d'une procédure relativement complexe qui souffrira d'un nombre croissant de demandes.

Les autorités européennes de protection des données réunies au sein du G29 ont, quant à elles, confié au sous-groupe « Futur de la vie privée » du G29 l'analyse des conséquences de l'arrêt de la CJUE. Le sous-groupe a défini des lignes directrices pour permettre aux autorités européennes de protection des données d'adopter une approche commune dans la mise en œuvre pratique de cet arrêt[240]. Grâce à ces lignes directrices, les autorités pourront coordonner leurs

[239] L. Marino, *Ibid*.

[240] Guidelines on the implementation of the court of justice of the european union judgment on "Google Spain and inc v. Agencia española de protección de datos (AEPD) and Mario Costeja González", 26 nov. 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf et C-131/12http://www.cnil.fr, nous y reviendrons s'agissant de l'effectivité du droit.

réponses aux plaintes qui leur sont adressées lorsque des moteurs de recherche ne donnent pas suite favorable à une demande d'effacement.

Il est à noter que la décision de la CJCE a déjà reçu un écho dans la jurisprudence française puisque le tribunal de grande instance de Paris a rendu le 19 décembre 2014, une décision enjoignant au célèbre moteur de recherche de retirer un lien de ses résultats de recherche[241]. Google est donc condamné pour avoir ignoré la demande de déréférencement de l'intéressée fondée sur le droit à l'oubli, demande qui visait un article relatant sa condamnation, en 2006, pour escroquerie. Elle faisait valoir que la présence de ce lien dans les résultats de recherche liés à son nom nuisait à sa recherche d'emploi. Lors d'une première tentative de retrait, elle avait utilisé le nouveau formulaire de droit à l'oubli de Google. En septembre 2014, sa demande a été rejetée, le moteur de recherche jugeant l'article d'intérêt public. Le tribunal s'est notamment appuyé sur l'ancienneté de l'affaire puisqu'il s'est écoulé près de 8 ans entre la publication de l'article et le dépôt de la plainte et a considéré que la demanderesse justifiait de « raisons prépondérantes et légitimes prévalant sur le droit à l'information ». On soulignera, à la lumière des développements consacrées au casier judiciaire que le juge a également retenu que cette condamnation pour escroquerie ne figurait pas sur le bulletin n°3 du casier judiciaire de la plaignante, et n'avait donc pas sa place dans les résultats de recherche de Google.

Il est à noter que, parallèlement, Google a mis en place un comité consultatif qui a effectué un tour de plusieurs grandes villes d'Europe afin de dégager une ligne de conduite dans la mise en œuvre des demandes d'effacement. Ces consultations ont donné lieu à un rapport[242] qui définit des critères permettant de décider de l'effacement. Le comité invite à tenir compte du rôle joué par le citoyen dans la vie publique, de la nature de l'information, de la source de l'information (journalistiques, gouvernementales, blogueurs réputés, etc.) et enfin, du temps qui peut rendre une information moins pertinente qu'au moment de sa divulgation ou au contraire, plus pertinente, si elle concerne une personne qui compte désormais sur la scène publique. Ces critères n'apportent pas réellement de nouveauté dans le débat, sans doute parce qu'il n'est pas possible de donner, *a priori*, des solutions précises. Chaque demande s'inscrit dans un contexte qui lui est propre et la généralisation d'une solution paraît difficile à envisager.

[241] TGI de Paris, ord. de référé du 19 déc. 2014, Marie-France M. / Google France et Google, Inchttp://www.lefigaro.fr/secteur/high-tech/2015/01/16/01007-20150116ARTFIG00005-google-condamne-pour-la-premiere-fois-en-france-sur-le-droit-a-l-oubli.php.

[242] The advisory council to Google on the right to be forgotten, 6 fév. 2015, https://drive.google.com/file/d/0B1UgZshetMd4cEI3SjlvV0hNbDA/view?pli=1

2.2.3.2. La responsabilité du moteur de recherche dans le référencement d'informations constitutives d'un contenu illicite

On peut également être amené à considérer que l'information contenue sur la page *web* est un contenu illicite parce qu'elle porte atteinte à la vie privée, qu'elle constitue une injure ou une contrefaçon par exemple. C'est alors la présence d'un contenu illicite sur la toile qui devrait être sanctionnée et qui en justifierait le retrait. Dans ce cas, la victime peut agir sur le fondement de la responsabilité délictuelle en prouvant la faute, le préjudice et le lien de causalité mais elle ne parviendra pas toujours à identifier l'auteur du contenu illicite. Elle peut alors se retourner contre les intermédiaires techniques, l'hébergeur ou le moteur de recherche, mais éprouvera les plus grandes peines à établir une quelconque faute de leur part. C'est pourquoi la victime agira le plus souvent sur le fondement de la LCEN en actionnant l'éditeur, l'hébergeur, ou le moteur de recherche. La responsabilité de ce dernier doit néanmoins être conciliée avec l'absence d'obligation générale de surveillance des contenus circulant sur Internet, ce qui explique que la jurisprudence ait parfois recours au concept générique de droit à l'oubli pour justifier ses décisions.

2.2.3.2.1. Une responsabilité à concilier avec l'absence d'obligation générale de surveillance des contenus

Il est plus aisé d'admettre la responsabilité des intermédiaires techniques lorsque le contenu dont se plaint la victime est illicite mais une action contre le moteur de recherche n'est pas sans inconvénient. Le 6 Novembre 2013, le TGI de Paris a rendu une ordonnance dans l'affaire opposant Max Mosley à Google images. Condamné dans un premier temps au retrait immédiat de clichés représentant le Président de la fédération internationale automobile dans des scènes d'intimité sexuelle, Google s'était exécuté. Toutefois, le demandeur constata une nouvelle publication des photos litigieuses sur Google Images et procéda à une mise en demeure de retirer les clichés. Google refusa en invoquant le fait qu'il n'avait pas à «faire la police sur Internet» et en se prévalant de « l'absence pesant sur lui d'une obligation de surveiller *a priori* les contenus qu'il indexe ». C'est ce refus qui conduit Max Mosley à saisir le juge des référés pour obtenir le déréférencement définitif des photos litigieuses sur le moteur de recherche. Le tribunal retient la responsabilité de Google, le condamne à 1 € symbolique et décide de l'exécution provisoire de la décision. Il interdit également à la société Google l'affichage des

clichés litigieux sur son moteur de recherche pendant une durée de 5 ans[243]. Selon le TGI, la mise en jeu de la responsabilité du moteur de recherche est justifiée par son refus de supprimer les clichés litigieux qui figuraient sur le moteur de recherche alors qu'il savait que ces publications portaient atteinte à la vie privée du demandeur.

La position est audacieuse et peut ne pas sembler tout à fait conforme à celle de la Cour de cassation en matière de contenu illicite et spécialement, d'images contrefaisantes, non pas en ce qu'elle condamne Google au retrait des clichés mais en ce qu'elle lui impose une désindexation pour l'avenir. Par plusieurs décisions, en effet, la haute juridiction a censuré les juges du fond qui avaient soumis la société Google à une obligation générale de surveillance des images qu'elle stocke et de recherche des reproductions illicites[244]. La CJUE a rendu des décisions allant dans le même sens. C'est le cas de l'arrêt du 16 février 2012 dont il résulte que les règles des États membres « doivent notamment respecter l'article 15, paragraphe 1, de la directive 2000/31, qui interdit aux autorités nationales d'adopter des mesures qui obligeraient un prestataire de services d'hébergement à procéder à une surveillance générale des informations qu'il stocke »[245]. La seule réserve au principe de l'article 6-I-2 de la LCEN réside en effet dans les contenus portant sur l'apologie du crime, d'incitation à la haine raciale ou encore de pornographie enfantine.

Il est à noter que, dans cette affaire, une décision avait qualifié le contenu d'illicite car attentatoire à la vie privée. Or, cette circonstance ne suffit pas toujours face à la liberté d'expression. La Cour européenne des droits de l'homme, qui s'était déjà prononcée dans cette affaire, avait fait prévaloir la liberté d'expression sur la violation de la vie privée en refusant d'ordonner à l'éditeur d'une publication en ligne d'effectuer le retrait de l'information dommageable sur Internet. Elle avait néanmoins décidé que le fait de publication devait donner lieu à une réparation en faveur de la victime du contenu illicite[246].

Une recommandation du Forum des droits de l'Internet[247], invitait à considérer que le moteur de recherche, informé de l'existence des pages illicites, doit procéder à leur

[243] Le juge retient la responsabilité de Google Incorporation dont le siège social est en Californie et met Google France hors de cause probablement parce que l'activité de cache des photos s'effectue aux USA. Voir en ce sens, A. Chéron, « Affaire Mosley / Google : liberté d'expression, atteinte à la vie privée et droit à l'oubli numérique », D. act. Nov. 2013.
[244] Civ. 1re, 12 juill. 2012, nos 11-15.165 et 11-15.188, D. 2012. 2075, obs. C. Manara ; *ibid*. 2071, concl. C. Petit ; *ibid*. 2331, obs. L. d'Avout et S. Bollée ; *ibid*. 2343, obs. J. Larrieu, C. Le Stanc et P. Tréfigny ; *ibid*. 2836, obs. P. Sirinelli ; *ibid*. 2013. 1503, obs. F. Jault-Seseke ; Rev. crit. DIP 2013. 607, note L. Usunier ; RTD com. 2012. 771, obs. F. Pollaud-Dulian ; *ibid*. 775, obs. F. Pollaud-Dulian ; *ibid*. 780, obs. F. Pollaud-Dulian.
[245] CJUE 16 févr. 2012, aff. C-360/10, Sabam c.Netlog, D. 2012. 549, obs. C. Manara ; *ibid*. 2343, obs. J. Larrieu, C. Le Stanc et P. Tréfigny ; *ibid*. 2836, obs. P. Sirinelli ; RSC 2012. 163, obs. J. Francillon ; RTD eur. 2012. 957, obs. E. Treppoz.
[246] CEDH 10 juillet 2011, n° 48009/08, Mosley c/ Royaume-Uni, JCP G 2011, 659, obs. G. Gonzalez et 16 juill. 2013, n°33846/07, W. et S. c. Pologne.
[247] Forum des droits de l'Internet, « Quelle responsabilité pour les créateurs d'hyperliens vers des contenus illicites ? », Recomm. rendue publique, 23 oct. 2003.

déréférencement, à charge pour la victime de faire une demande en ce sens qui soit « précise et sérieuse, de telle manière qu'elle puisse être traitée par le créateur d'hyperliens »[248]. Le Forum recommandait d'ailleurs « aux victimes de contenus préjudiciables d'agir préalablement contre l'auteur direct de ce contenu (l'éditeur d'un site web, l'auteur d'un message...) et, dans les limites prévues par la loi, contre son hébergeur, lorsque l'un ou l'autre est facilement identifiable et atteignable »[249]. Il estimait « souhaitable, lors de toute demande de déréférencement adressée à un moteur de recherche, que la victime apporte auprès de l'exploitant de moteur de recherche la preuve qu'elle est intervenue ou qu'elle a tenté d'intervenir contre l'éditeur et/ou l'hébergeur du site »[250]. C'était bien le cas dans l'affaire Mosley mais il est vrai que la sanction retenue par le juge des référés fait peser sur le moteur de recherche une obligation plus lourde qu'il y paraît puisqu'il ordonne de veiller à la non réapparition des images pendant 5 ans. Pareille sanction aboutit à mettre à sa charge une obligation de surveillance des contenus. D'un autre côté, on peut s'étonner du caractère provisoire de la sanction car rien ne permet de douter du caractère attentatoire de ces photos à la vie privée de la victime et le temps n'enlèvera rien à ce caractère. Cela traduit sans doute la volonté du juge de ne pas entrer dans le débat sur le droit à l'oubli numérique et nous conduit à considérer que la LCEN n'est probablement pas le fondement le plus adéquat.

2.2.3.2.2. La caractérisation d'un contenu illicite par la référence au droit à l'oubli

C'est également sur le fondement de l'article 6.I.2 de la loi du 21 juin 2004 que s'était appuyé le TGI de Paris pour condamner le moteur de recherche Google mais le raisonnement différait quelque peu de celui mené dans l'affaire Max Mosley. Est relevé, l'atteinte au droit à la vie privée d'une femme ayant participé à une vidéo pornographique sous un pseudonyme et dont le véritable nom patronymique était associé à des sites pornographiques alors qu'elle avait tourné cette page de sa vie depuis plusieurs années[251]. En l'espèce le juge a caractérisé le trouble manifestement illicite en incluant une référence directe au droit à l'oubli. Le juge retient en effet que « si Mme Z. lorsqu'elle a tourné ce film, a accepté nécessairement une certaine distribution même si ensuite elle n'a pas *a priori* consenti à sa numérisation et à sa diffusion sur Internet et si cette vidéo ne révèle pas en elle-même des scènes de sa vie privée, il n'en demeure pas moins que ce film témoigne à une époque donnée de la vie de la jeune femme laquelle entend bénéficier du droit à l'oubli ».

[248] Recomm. préc., p. 15.
[249] *Ibid*.
[250] Recomm. préc., p. 8.
[251] TGI Paris, réf., 15 févr. 2012, Diana Z. c/ Google : www.legalis.net, Comm. com. électr. n° 5, Mai 2012, comm. 54, A. Lepage.

On peut ici s'interroger sur la réalité de l'atteinte à la vie privée et sur la pertinence du fondement textuel de la mise en œuvre de la responsabilité. Pourrait-on admettre qu'une personne, actrice de films pornographiques, travaillant sous un pseudonyme, s'oppose à ce que son nom patronymique soit cité par des tiers pour cette activité (y inclus des journalistes) ? En principe, la seule révélation du nom peut constituer une atteinte à la vie privée dans la mesure où l'on peut considérer que, en choisissant d'exercer sous un pseudonyme, la personne exprime clairement qu'elle ne veut pas que son nom patronymique soit utilisé dans la sphère professionnelle. En outre, le droit considère que la personne a une propriété exclusive sur ce pseudonyme. La situation serait toute autre si elle exigeait que le pseudonyme lui-même ne soit plus utilisé ou référencé en raison de l'association du pseudonyme à une activité dont elle veut « tourner la page ». En outre, si dans ses connaissances, une personne la reconnaissait, il serait tout à fait légitime, au nom de la liberté d'expression, que cette personne puisse révéler son nom patronymique au public.

La décision du 28 octobre 2010 précitée avait également tranché sur le fondement du droit au respect de la vie privée[252] mais fournissait peu d'éléments, ce que l'on peut regretter. En particulier, rien n'était dit sur le contexte dans lequel avait été tournée la vidéo, professionnel ou amateur, ce qui impacte de manière pourtant significative la qualification de l'atteinte. En effet, dans le premier cas, on peut considérer que tout participant est nécessairement consentant à une distribution, même si l'on peut imaginer certaines restrictions. Dans le second cas, on peut imaginer beaucoup plus de réserves à une distribution car ce n'est pas nécessairement sa finalité. De même, l'acteur d'un film professionnel, quelle qu'en soit sa nature, n'est pas censé livrer des éléments de sa vie privée lorsqu'il joue alors que celui qui participe à un film amateur peut parfaitement livrer des éléments de sa privée. Il est vrai que, comme l'avait souligné le juge, la participation à une vidéo pornographique en tant qu'actrice peut être considérée comme faisant partie de sa vie privée parce qu'il témoigne d'une époque particulière de sa jeunesse[253]. Mais si un tel raisonnement devait se généraliser, les producteurs de films pornographiques auraient du souci à se faire… Il semble que la reconnaissance de l'atteinte à la vie privée soit très discutable dans cette affaire surtout si l'on considère que le film était professionnel. Mettre en jeu la responsabilité de l'auteur du contenu, de l'hébergeur ou du moteur de recherche comme le suggèrent certains, présuppose dans le contexte juridique actuel, que le contenu soit illicite. Or, dans le cas où la personne a accepté de participer à un film devant faire l'objet d'une diffusion, la présence de ce film sur la toile n'est pas une atteinte au droit à la vie privée. Ce n'est pas tant la présence du film sur la toile qui est illicite mais bien le fait qu'en utilisant le

[252] TGI Montpellier, ord. Réf, 28 oct. 2010, Comm. Comm. Électr. n°5, Mai 2011, comm. 47, A. Lepage.
[253] A. Lepage, *Ibid*.

nom de la personne concernée, autrement dit, une donnée à caractère personnel, l'internaute accède très facilement au site abritant la vidéo. Dès lors, la situation n'est pas très éloignée de celle qui a été soumise à la CJUE dans l'affaire Google Spain contre AEPD. C'est implicitement un droit à l'oubli qui justifie la condamnation du moteur de recherche en tant que responsable de traitement car c'est son activité propre qui génère un préjudice. On pourrait rétorquer que dans ce cas de figure il n'y a pas là de dysfonctionnement du moteur de recherche, il assure la fonction qu'il doit assurer. C'est vrai. *A priori* seulement. En effet, il est *a priori* normal que le moteur de recherche fasse le lien entre le nom d'une actrice et le film auquel elle a participé. On admettra tout de même, si l'on veut bien un bref instant se mettre dans la peau d'un spectateur intéressé par le genre, que la qualité des acteurs n'est pas, à de rares exceptions près sans doute, le critère de sélection de ce type de vidéo. De la même manière, accéder à une annonce de vente forcée en recherchant des éléments de profil d'une personne sur qui l'on se renseigne « à toutes fins utiles » satisfait sans doute une certaine curiosité mais constitue en réalité une sorte de profilage parfois malsain (quand il est fait par la banque auprès de laquelle la personne veut emprunter ou de l'employeur qui cherche à recruter).

Même dans l'hypothèse où le contenu peut être qualifié d'illicite comme portant atteinte à la vie privée, on peut considérer que le rôle du moteur de recherche n'est pas négligeable car de la même manière, sans l'indexation qui lie le nom de la personne au contenu, la seule présence du contenu sur la toile est peu préjudiciable.

Pour terminer sur le champ des débiteurs d'un droit à l'oubli, il convient de préciser que le paragraphe 2 de l'article 17 de la proposition de règlement prévoit que lorsque le responsable du traitement « **a rendu publiques** les données à caractère personnel sans aucune justification fondée sur l'article 6, paragraphe 1, il prend toutes les mesures raisonnables pour procéder à l'effacement de ces données, y compris par des tiers, sans préjudice de l'article 77. Le responsable du traitement informe la personne concernée, lorsque cela est possible, des mesures prises par les tiers concernés ». Le texte vise un type de traitement bien précis : **la diffusion des données**. C'est le traitement qui, selon nous, est au cœur de la problématique du droit à l'oubli. D'une part, telle qu'elle est envisagée, la responsabilité du responsable de traitement ou du tiers, dans ce contexte, est loin d'être absolue. Il contracte une obligation de moyens ce qui n'offre à la personne concernée qu'un droit limité. D'autre part, la rédaction diffère de celle de la proposition initiale et l'on peut en déduire quelques conséquences. Il était notamment prévu que lorsque le responsable de traitement avait autorisé un tiers à publier des données à caractère personnel, il était considéré comme responsable de cette publication. Dans la nouvelle version,

il n'est plus fait de référence à une quelconque autorisation du responsable de traitement ce qui pourrait conduire à considérer que sa responsabilité est engagée même s'il n'a pas autorisé le tiers à publier les données. Pareille interprétation conduit inexorablement à une extension de la responsabilité du responsable de traitement assortie il est vrai d'une sérieuse modération. En effet aux « mesures *raisonnables* » s'ajoute une information de la personne concernée, *lorsque cela est possible*, des mesures prises par les tiers concernées ».

Le texte prend la mesure des effets d'une divulgation massive permise par le transfert de données par le responsable de traitement à des tiers. Il facilite l'action des personnes concernées contre les responsables et, en cela, doit être approuvé.

Néanmoins, les procédures, réglementations et, surtout, l'obsession de la protection des données privées de l'Union Européenne percute de plein fouet un principe quasi absolu du droit américain : la liberté d'expression[254]. Pour Eric Schmidt, président exécutif de Google, il y a « un équilibre entre le droit à l'oubli et le droit de savoir ». Les Européens « sont du mauvais côté » du point d'équilibre, selon lui[255]. A Paris, une nouvelle initiative, l'Open Internet Project, a réuni presque 400 acteurs européens de l'Internet, qui menace de poursuivre Google pour abus de position dominante[256].

Pour conclure cette deuxième partie, deux constats s'imposent. D'une part, la diversité des données et des acteurs concernés par un possible droit à l'oubli induit le recours à des mécanismes divers de protection de la personne. Ainsi, pour les données particulièrement sensibles quant à leur nature, le législateur organise des dispositifs spéciaux de protection. C'est le cas pour les données médicales, judiciaires ou touchant l'état et la situation personnelle et sociale de la personne dont l'accès est contrôlé soit par un accès limité, soit par des mesures d'anonymisation, soit encore et plus radicalement, par l'effacement des données sous contrôle judiciaire. S'agissant des autres données, en libre accès, le législateur instaure soit des restrictions à l'utilisation comme c'est le cas pour l'employeur – mais nous avons néanmoins souligné le caractère illusoire de telles restrictions – soit la possibilité d'en obtenir le retrait ou l'effacement, soit encore, et c'est là une interprétation jurisprudentielle du dispositif de protection des données – d'obtenir un déréférencement de telle sorte que la donnée demeure mais que son accès à partir du nom de la personne n'est plus possible.

D'autre part, on soulignera l'extrême souplesse des dispositions de protection de la vie privée et des données à caractères personnel qui peuvent couvrir des champs nouveaux du

[254] Voir sur ce point, W. J. Maxwell, « La jurisprudence américaine en matière de liberté d'expression sur Internet », *in* Conseil d'Etat, *Le numérique et les droit fondamentaux*, Les rapports du Conseil d'Etat, sept. 2014
[255]http://www.lemonde.fr/idees/article/2014/05/18/google-n-est-pas-pres-d-oublier-l-europe_4420884_3232.html
[256] *Ibid*.

marché du numérique pour lesquels ils n'avaient pourtant pas été conçus. Plus fondamentalement, en atteignant les moteurs de recherche, la jurisprudence donne au régime de protection des données personnelles un large rayonnement et aux personnes concernées, une arme nouvelle. Elle permet, à notre sens, d'étendre la notion de traitement illicite à une activité qui est au cœur de la problématique d'un droit à l'oubli et qui, jusqu'alors, était considérée comme licite en soi. Naturellement, l'idée de droit à l'oubli est sous-jacente mais sa consécration, en tant que droit autonome, n'est pas indispensable parce qu'il n'y a pas de « forçage » d'une catégorie juridique préexistante. Cela ne signifie pas qu'elle n'est pas souhaitable. Il nous semble en effet que de proche en proche, le droit à l'oubli devient un concept générique couvrant différents dispositifs techniques concourant à la protection de la personne et dont la mise en œuvre peut favoriser la tranquillité de la personne et limiter les intrusions malsaines dans sa vie – privée *a priori* mais cette caractéristique passe désormais au second plan. Qu'un tel droit soit souhaitable ne signifie pas pour autant que son effectivité puisse être garantie, c'est ce que nous devons nous attacher à vérifier**.**

III. L'EFFECTIVITE DU DROIT A L'OUBLI

Dans la détermination des contours d'un droit à l'oubli, l'accent a été mis sur le fait qu'un tel droit pouvait se matérialiser de différentes manières, notamment : effacement, anonymisation, déréférencement et limitation de l'accès aux données. Ces techniques sont séduisantes mais sont-elles réalistes ? Les notions d'oubli et d'oubli numérique abordées en introduction ont permis de mettre en évidence que pour un être humain, la mémorisation d'une information demande souvent un effort conscient de sa part, alors que l'oubli est un phénomène naturel qui intervient inconsciemment. Par contraste, les ordinateurs étant conçus pour stocker (et traiter) de l'information, le fait d'oublier constitue un défi technique. En effet, contrairement au cerveau humain, les ordinateurs ne disposent pas *a priori* de mécanismes permettant d'introduire des priorités en favorisant certaines informations par renforcement, alors que d'autres sont effacées peu à peu. D'un point de vue juridique, les approches précédentes ont permis de déceler un certain nombre de réserves à l'affirmation d'un droit à l'oubli. En effet, la consécration d'un droit nouveau et autonome se heurterait à certaines limites liées à l'environnement dans lequel un tel droit devrait s'inscrire.

L'effectivité d'un droit à l'oubli doit donc pouvoir se mesurer à un double niveau : technique, d'une part(1), juridique, d'autre part (2). C'est donc ici l'environnement technico-juridique qui retiendra notre attention et nous permettra d'apprécier le caractère réaliste d'un tel droit.

1. MODALITES TECHNIQUES D'EXECUTION DU DROIT A L'OUBLI

À l'échelle d'une machine unique, il est déjà très difficile de faire disparaître une information de manière efficace si elle a été stockée sur un disque dur standard sans précautions particulières. En effet, même si la possibilité de supprimer un fichier existe dans la plupart des systèmes d'information, il s'agit d'une fonctionnalité simpliste qui ne peut pas être considérée comme un oubli total et définitif. En pratique, la suppression d'un fichier consiste généralement en l'effacement d'une entrée dans une table d'indexage. Il ne s'agit donc pas d'un écrasement réel de la donnée elle-même. De plus, pour être effectif, l'écrasement d'une zone mémoire sur un disque dur à stockage magnétique est un processus qui doit être répété de nombreuses fois pour s'assurer que les données ne seront plus lisibles. Pour réaliser cet effacement, il existe des logiciels dédiés qui sont par exemple référencés dans les listes de produits certifiés (selon les

« Critères Communs »[257] ou la « Certification de Sécurité de Premier Niveau »[258]) par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Ces logiciels, appelés outils *anti-forensiques*, sont souvent utilisés lorsqu'un risque spécifique relatif à la rémanence des données est identifié, comme par exemple lors du remplacement d'un disque dur contenant des données sensibles. Cependant, la majorité des systèmes d'information s'appuie sur une suppression simple, qui n'offre aucune garantie efficace lorsqu'une investigation numérique est conduite sur le contenu du disque dur (aussi appelée analyse *forensique*).

Même si le risque de persistance de l'information lié aux supports de stockage eux-mêmes est un risque bien réel, il n'est pas en général celui qui inquiète le plus le public lorsque la question du droit à l'oubli est abordée[259]. Actuellement, le risque le plus prégnant et le plus difficile à résoudre techniquement est celui lié à l'interconnexion des systèmes d'information et des réseaux d'ordinateurs. Le développement d'Internet a conduit à la collection de données *via* des applications et protocoles qui les diffusent ensuite dans la Toile ainsi qu'à l'émergence de verrous technologiques majeurs par rapport à la sécurité informatique et au respect de la vie privée. Ainsi, un verrou majeur concerne *le traçage et le contrôle du devenir d'une donnée une fois qu'elle a été transmise à un tiers*. Plus particulièrement, lors de la mise en œuvre technique du droit à l'oubli, il semble important de pouvoir garantir qu'une entité distante a réellement supprimé une donnée qui lui a été confiée, sans préalablement en avoir fait de copies et sans l'avoir transmise à un tiers. Malheureusement, au vu de l'architecture actuelle d'Internet, il n'existe aucun mécanisme technique qui peut dans l'absolu offrir une telle garantie sur la copie ou la conservation possible d'une donnée. Considérons par exemple un interlocuteur distant qui a un accès licite à une information sous la forme d'un texte ou d'une image affichée sur son écran. Même si au niveau de son ordinateur un mécanisme est mis en place pour lui interdire de faire une copie de cette donnée, il lui est toujours possible de prendre une photographie de son moniteur *via* un appareil indépendant de son ordinateur. Ensuite, cet interlocuteur pourra faire ce qu'il veut de la copie obtenue.

Cette simple observation exclut de pouvoir proposer une mise en œuvre du droit à l'oubli sur des données numériques qui serait à la fois totalement générique et parfaitement effective. Cependant, ce résultat qui s'appuie sur un scénario relativement spécifique ne doit pas condamner toute démarche dans ce sens. En particulier, il reste possible de concevoir des implémentations techniques (partielles) du droit à l'oubli, se basant sur des solutions logicielles,

[257] ANSSI, *Produits certifiés CC*, http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-certifies-cc/
[258] ANSSI, *Produits certifiés CSPN*, http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-certifies-cspn/
[259] Ceci ne présuppose rien quant à l'importance réelle de ce risque. En particulier, le grand public est souvent très peu conscient des risques informationnels liés à la vente d'occasion d'un disque dur ou d'un ordinateur. Ainsi un acquéreur, pour peu qu'il possède quelques connaissances techniques (limitées), pourra avoir accès à une grande quantité de données personnelles ou sensibles que le vendeur pensait avoir supprimées en « vidant la poubelle » de son ordinateur.

matérielles ou même une combinaison des deux, pouvant sous certaines conditions, fournir à un individu un certain niveau de garantie sur la suppression de données dont il est à l'origine ou le concernant. Les approches que nous présentons ci-après sont des exemples de telles solutions. En particulier, elles sont capables, si certaines hypothèses sont vérifiées, de garantir la disparition d'une donnée dans le cadre de contextes ou d'applications particulières. Une hypothèse qui est souvent faite est qu'il n'est pas possible de faire une copie d'une donnée d'une manière comparable à l'exemple de l'appareil photo mentionné précédemment ou de faire transiter des informations à l'extérieur du système d'information considéré. Cette hypothèse est contraignante et irréaliste de manière générique, empêchant ainsi toute garantie forte, mais peut néanmoins être valide pour les scénarios où le risque de malveillance et les enjeux sont faibles.

Pour un chercheur en sécurité et protection de la vie privée, un modèle d'adversaire plus réaliste est de considérer que si un individu ou une entité (qu'on appellera ci-après l'adversaire) a eu un accès légitime à la donnée par le passé alors il n'existe aucun moyen technique imparable pour l'empêcher de faire une copie de cette donnée (et donc aussi de la diffuser). Par contre, une fois qu'une date d'expiration prédéfinie a été dépassée, on peut s'assurer qu'il devient alors impossible à l'adversaire d'accéder à toute donnée pour laquelle il n'a pas activement décidé de faire de copie par le passé. Autrement dit, l'adversaire doit à l'avance choisir les données pour lesquelles il souhaite empêcher le droit à l'oubli d'être effectif. Par contre, pour les données pour lesquelles il n'a pas été proactif, on peut garantir grâce à des moyens techniques qu'il ne pourra pas empêcher leur effacement une fois la date prédéfinie dépassée. Ce modèle peut sembler relativement faible par rapport à d'autres mais il a l'avantage d'être réalisable par les techniques présentées ci-après.

Il existe donc différentes techniques permettant de contribuer à la mise en œuvre d'un droit à l'oubli. Ainsi en est-il de l'anonymisation des données et des solutions technologiques qui permettent de s'assurer qu'une donnée disparaîtra effectivement d'elle-même d'un système donné (indépendamment des copies qui ont pu en être faites), soit au bout d'un certain temps, soit sur demande d'une personne donnée[260].

En particulier, on peut distinguer trois grandes familles d'approches. La première famille est constituée des techniques permettant que la donnée disparaisse toute seule au bout d'un certain temps alors que la deuxième famille prévoit que l'effacement se fera sur demande d'une personne donnée. Enfin, la dernière famille vise à rendre inaccessible une donnée même si celle-ci ne peut pas être effacée. Nous présenterons ci-après un panorama de quelques-unes

[260] Nous présenterons un panorama de quelques-unes des technologies qui nous semblent prometteuses en vue de permettre une implémentation (partielle et limitée) du droit à l'oubli.

des technologies qui nous semblent prometteuses en vue de permettre une implémentation (partielle et limitée) du droit à l'oubli.

1.1. L'anonymisation : une technique aux effets limités

Pour les responsables de traitement, la notion de droit à l'oubli fait écho à l'obligation de supprimer les données à caractère personnel qui ne sont plus absolument nécessaires à la finalité pour laquelle elles ont été collectées. Dans certains cas, nous l'avons vu, il est cependant permis[261] de conserver ces données en vue d'un traitement à des fins historiques, statistiques ou scientifiques. Théoriquement, on peut aussi *anonymiser* certaines données, en retirant toute référence à la personne concernée, de manière à ce qu'elles ne constituent plus des données à caractère personnel au sens strict de la loi mais conservent néanmoins une utilité statistique (et donc une valeur économique pour l'entité les ayant collectées). La plupart des fournisseurs de services qui tirent la majeure partie de leurs revenus de la vente et l'exploitation de données personnelles préfèrent d'ailleurs en général avoir recours à une anonymisation de données collectées que de procéder à leur suppression directe.

Plusieurs incidents se sont succédé depuis une quinzaine d'années qui remettent en cause l'effectivité même du principe de l'anonymisation de données, en démontrant en particulier que ce processus permet rarement de couper réellement le lien entre une personne et les informations qui la concernent. Ainsi même si dans une base de données particulière on ne retrouve plus directement, ce qui est appelé « informations directement nominatives » dans la version d'origine de la loi « Informatique et Libertés » (ou encore *Personally Identifiable Information* par le droit américain), un recoupement des informations « anonymisées » reste possible avec d'autres bases de données existantes. La « désanonymisation » résultant de ce recoupement pourra potentiellement conduire à la ré-identification totale ou partielle des personnes physiques auxquelles il était fait référence. Un exemple historique de désanonymisation concerne le *Massachusetts Group Insurance Commission* qui a publié à la fin des années 90 les données médicales « anonymisées »[262] des agents de l'Etat. Latanya Sweeney, alors étudiante en informatique, avait réussi à chaîner les données publiées avec la liste des votants de cet Etat (liste qui est publique ou vendue pour un montant modique aux États-Unis) en utilisant pour cela des attributs tels que le sexe, la date de naissance et le code postal, qui semblent anodins pris de manière individuelle mais qui combinés ensemble jouent le rôle de *quasi-identificateurs*. Latanya Sweeney a ensuite pu envoyer au gouverneur de l'Etat

[261] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, art. 36.
[262] Plus précisément, le processus d'anonymisation consistait à enlever le nom et le prénom de chacun des individus présents dans l'ensemble de données ainsi que tout identifiant unique comme le numéro de sécurité sociale ou encore l'adresse précise.

son propre dossier médical, suite à quoi l'Etat est revenu sur la publication de ces données. Poursuivant sa démarche, Sweeney a ensuite montré en 2000 que 87 % des Américains étaient identifiables de manière unique par la combinaison des attributs mentionnés ci-dessus, attributs qui sont en général dévoilés sans problème lors de sondages « anonymes ». Afin de résoudre ce problème, Sweeney a ensuite développé le concept de *k*-anonymité[263], qui est à la fois une méthode d'anonymisation procédant par généralisation (en révélant par exemple la tranche d'âge plutôt que l'âge précis) et suppression des données ainsi qu'une mesure du « degré d'anonymat » [264] de la base de données résultant du processus d'anonymisation.

D'autres incidents plus récents, tels que l'affaire de la publication des requêtes des utilisateurs par AOL ou la ré-identification des clients de Netflix, ont confirmé que l'anonymisation de données personnelles ne constituait pas une protection suffisante contre la ré-identification des personnes[265]. Ces travaux permettent également une lecture différente de la définition des données à caractère personnel présente dans l'article 2 de la loi « Informatique et Libertés », dont en particulier la dernière phrase du premier paragraphe qui dispose : « *Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne* ». Avec le recul, cette définition semble particulièrement pertinente et bien formulée car elle couvre un risque technique inconnu au moment de sa rédaction, mais elle est aussi très difficile à appliquer du fait de son caractère extrêmement général. Ainsi, de fait, n'importe quelle information, même si elle semble *a priori* anodine, peut potentiellement servir à identifier un individu. Par exemple dans le cas de Netflix, les informations permettant d'identifier un individu étaient les notes données à des films. En pratique, il est très difficile d'évaluer le niveau d'anonymat offert par une méthode d'anonymisation particulière à l'aide d'une métrique suffisamment générique pour couvrir toutes les inférences qui pourraient être faites par un adversaire accédant à la version anonymisée des données. En particulier, ce niveau d'anonymat dépend des ressources accessibles à l'adversaire, dont en particulier les connaissances additionnelles qu'il possède, ce qui demande par exemple de pouvoir modéliser les sources d'information auxquelles il a accès ou auxquelles il pourra avoir accès dans le futur.

---

[263] L. Sweeney, « k-Anonymity: A Model for Protecting Privacy », *in* International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2002, vol. 10, pp. 557-570.

[264] Plus précisément dans le modèle de la *k*-anonymité, la base de données qui sera publiée sera telle que chaque individu de la base originelle est garanti de se retrouver dans un groupe où au moins *k-1* autres individus auront le même profil. Ainsi, le paramètre *k* peut être considéré comme une mesure du niveau de vie privée fournie par la publication de la version *k*-anonymisée de l'ensemble de données.

[265] P. Ohm, *Broken promises of privacy : responding to the surprising failure of anonymization*. In 57 UCLA Law Review 1701, 2010.

Globalement, d'un point de vue technique, à l'aune des résultats actuels de l'état de l'art, l'anonymisation de données ne semble donc pas une réponse satisfaisante pour offrir une mise en place effective du droit à l'oubli. Il n'en reste pas moins vrai que, pour le juriste, c'est une technique à ne pas négliger parce que c'est un premier niveau de garantie à offrir aux usagers. En outre, il rend compatible la publication et la conservation des données avec le respect des droits de la personnalité. Naturellement, la mise en exergue des limites techniques de cette pratique doit être prise en compte pour considérer que si l'anonymisation est une possibilité, ce n'est pas une garantie absolue.

1.2. Le principe des politiques adhésives

Une manière classique de définir les utilisations et opérations possibles pouvait être faite sur une donnée à l'intérieur d'un système d'information est de lui associer une *politique de sécurité* spécifiant les traitements qu'il est permis, interdit ou obligatoire d'effectuer avec la donnée en question. L'applicabilité d'une politique de sécurité (appelée aussi parfois politique de confidentialité) va en général bien au-delà du droit à l'oubli, mais les conditions de conservation, de suppression ou d'altération d'une donnée sont des éléments qui peuvent y figurer. Les « politiques adhésives » (ou *sticky policies* en anglais)[266] poussent le concept encore plus loin en proposant de ne jamais séparer la donnée de la politique en question, même lorsque cette donnée devient mobile et est communiquée à travers un réseau informatique ou dans le cadre d'une application distribuée. Ainsi lorsqu'un fichier est transmis entre deux personnes, d'une machine à une autre ou entre différents programmes, la politique reste toujours associée à la donnée et en est indissociable. Pour que cette technique soit efficace, il faut que l'ensemble du système d'information dans lequel évoluent les données soit conçu pour comprendre et appliquer automatiquement ces politiques, ce qui constitue dans l'absolu une hypothèse très forte. Le principal verrou technologique consiste ici à s'assurer que ces politiques adhésives seront bien respectées. Grâce aux outils offerts par la cryptographie, il devient possible par exemple de s'assurer de l'authenticité d'une politique et du fait qu'elle n'ait pas été indûment modifiée depuis sa création.

Afin de s'assurer de l'application des politiques de sécurité, on peut introduire dans le système d'information des entités qui sont dites « de confiance ». Du point de vue de la sécurité, un élément est dit « de confiance » si l'on a besoin de faire l'hypothèse que cet élément se comporte de manière correcte pour avoir foi dans l'ensemble du système. Par exemple, lorsque

[266] G. Karjoth & M. Schunter, « A privacy policy model for enterprises », *in* 15th IEEE Computer Security Foundations Workshop, IEEE Computer Society Press, 2002.

l'on a recours à un tiers de confiance pour l'horodatage d'un document, on présuppose que ce tiers de confiance accomplit son travail de manière sincère et efficace afin d'accepter les garanties qui en découlent. En d'autres termes, les éléments de confiance sont des points critiques du système qui, s'ils violaient les règles de fonctionnement qui leur sont assignés, feraient s'effondrer les propriétés et caractéristiques de l'ensemble de l'application. A l'image des procédures mises en place par le droit français pour la certification des tiers de confiance pour l'horodatage, il convient donc bien sûr de s'assurer que les éléments de confiance sont fiables mais aussi de limiter au maximum leur importance. Ainsi, pour le cas naïf des politiques adhésives simples, on a besoin de faire l'hypothèse que l'ensemble du système d'information est « de confiance ». Autrement dit, il est nécessaire de croire à la fiabilité de l'ensemble des acteurs et des logiciels pour avoir la conviction que les politiques sont respectées.

L'informatique de confiance (*Trusted Computing* en anglais)[267] propose de s'appuyer sur des entités « de confiance » de type matériel qui sont particulièrement sûres. Plus particulièrement sur chaque machine concernée, une puce électronique appelée TPM (*Trusted Platform Module* en anglais) est installée dont le fonctionnement suit une spécification standardisée et est garanti par un tiers de confiance indépendant. Le TPM a la capacité de fournir à des interlocuteurs distants des garanties très fortes sur le fonctionnement de la machine sur laquelle il opère. En utilisant ce TPM comme brique de base, il devient possible de concevoir des architectures d'applications distribuées[268], dans lesquelles l'accès aux données est subordonné à la garantie que la politique adhésive va être respectée. En théorie, les garanties fournies par ce type d'architecture sont particulièrement fortes et difficiles à contrefaire. Cependant, lorsqu'on essaye de s'appuyer sur les technologies du *Trusted Computing* pour mettre au point un système de protection de la vie privée, il faut faire face à un grand nombre de défis techniques. Tout d'abord, la phase de certification des logiciels, qui permet de déclarer quels sont les services qui respectent une propriété particulière, est trop complexe pour qu'il soit envisageable de la mettre en place de manière sérieuse et fiable à large échelle. Une des conséquences pratiques probables serait une marchandisation simple de ces certificats (à la manière des certificats d'identité actuellement utilisés par le protocole HTTPS). Cet effet de marchandisation fragiliserait les garanties offertes et générerait une confiance indue des utilisateurs dans le système, ce qui pourrait rendre le remède pire que le mal car promettant un respect des politiques alors que ceci ne peut plus être garanti formellement. De plus, les technologies de type *Trusted Computing* constituent en elles-mêmes un risque pour la vie privée

[267] S. Pearson, « Trusted Computing Platforms: TCPA Technology », in Context, Prenctice Hall PTR, USA, 2002.
[268] M. Casassa Mont, S. Pearson & P. Bramhall, *Towards accountable management of identity and privacy: sticky policies and enforceable tracing services*. Rapport de recherche HP labs HPL-2003-49, Royaume-Uni, 2003.

des utilisateurs, en raison de leur autonomie et leur contrôle sur les machines en leur possession, ou encore pour la libre concurrence. Ces risques sont pointés depuis de nombreuses années par nombre de spécialistes en sécurité informatique[269], par le G29[270] ou même (de manière plus réservée) par des membres du consortium soutenant ces technologies[271]. Pour de nombreux chercheurs en protection de la vie privée, il semble évident que même si ce type de solution est un repère incontournable situé à une extrémité dans le spectre des approches possibles, il est plus raisonnable de rechercher des systèmes offrant des garanties moins fortes mais présentant aussi moins de risques et limitant aussi les hypothèses de confiance qui sont nécessaires.

1.3. Publication éphémère de données

Le principe de la *publication éphémère* consiste à concevoir des systèmes informatiques dans lesquels toute donnée qui est insérée va éventuellement disparaître, sans pour cela, requérir une action consciente de la part d'un utilisateur. Par exemple, il est possible de créer un système de publication éphémère qui exploite à son avantage l'aspect dynamique de certains systèmes informatiques qui les rend ces derniers difficilement prédictibles, afin d'effacer petit à petit les données stockées dans le système.

On pourrait ainsi imaginer mettre en place un système de courriel éphémère où une date d'expiration pourrait être incluse à tout courriel envoyé de telle manière que ce courriel disparaisse de lui-même une fois la date d'expiration passée. On peut aussi citer comme exemple *Snapchat*[272], qui est une application pour smartphone se basant explicitement sur le principe de publication éphémère. En particulier, l'objectif principal de cette application est de pouvoir partager des photos ou vidéos avec ses contacts du moment présent et de telle manière à ce que le contenu partagé s'efface automatiquement au bout de quelques secondes. Le principe lui-même est intéressant en tant qu'illustration concrète d'une forme partielle de droit à l'oubli mais la sécurité de cette application reste encore à améliorer.

Vanish[273] est un système permettant à une donnée de disparaître automatiquement au bout d'un certain temps sans requérir aucune action explicite de la part du possesseur de cette donnée. En un certain sens, cette donnée peut donc être considérée comme étant dotée de capacités d'autodestruction. Vanish est basée sur une architecture ouverte et décentralisée de type réseau pair-à-pair, dans laquelle les données sont stockées de manière distribuée au niveau

[269] R. Anderson, *Trusted Computing" frequently asked questions*, 2003 (http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html).
[270] Article 29 Data Protection Working Party, *Working document on Trusted Computing Platforms and in particular on the work done by the Trusted Computing Group (TCG group)*, 2004.
[271] S. Pearson, « Trusted Computing: Strengths, Weaknesses and Further Opportunities for Enhancing Privacy », *in* Proceedings of the Third International Conference on Trust Management (iTrust 2005), Springer Verlag, 2005, 3477, pp. 305-320.
[272] https://www.snapchat.com
[273] R. Geambasu, T. Kohno, A. A. Levy & H. M. Levy, « Vanish: Increasing data privacy with self-destructing data », *in* Proceedings of the 18th USENIX Security Symposium, 2009.

des nœuds du réseau. Plus précisément, le réseau pair-à-pair est organisé autour d'une structure de donnée appelée table de hachage distribuée (*Distributed Hash Table* ou *DHT* en anglais) qui permet d'associer à une donnée particulière une ou plusieurs positions dans le réseau. Lorsqu'un utilisateur veut insérer une donnée dans Vanish, le système chiffre cette donnée avec une clé générée aléatoirement et non connue de l'utilisateur, avant de fragmenter cette clé en plusieurs morceaux à l'aide d'un algorithme de « partage de secret »[274]. Le partage de secret est une primitive cryptographique permettant de morceler une information en *n* fragments de telle manière à ce que seule une connaissance d'au moins t fragments permet de reconstituer l'information originelle (*t* et *n* sont des paramètres pouvant être laissés au choix de l'utilisateur). Les fragments de cette clé sont ensuite disséminés dans le réseau en leur assignant une position pseudo-aléatoire dans la table de hachage distribuée avant d'effacer ensuite la copie locale de la clé. Du fait de la dynamique naturelle du réseau ouvert, des nœuds quittent et rejoignent régulièrement le réseau, induisant ainsi un brassage naturel qui est exploité de manière positive par Vanish pour s'assurer de la disparition effective des fragments de la clé (sans pour autant pouvoir fournir de garanties formelles sur la date réelle de disparition de l'information). En effet, on suppose que lorsque qu'un nœud quitte le réseau, il efface le contenu de sa mémoire et les fragments de clé qu'il avait en sa possession. Le fait de recourir à un réseau pair-à-pair permet aussi de distribuer la confiance sur plusieurs nœuds et un meilleur passage à l'échelle de cette solution.

Ephemerizer[275] est un ancêtre de *Vanish* dans lequel la gestion des clés est assurée par une entité centrale de confiance. Plus précisément, lorsqu'un utilisateur introduit une nouvelle donnée dans l'*Ephemerizer* celle-ci est chiffrée est chiffrée avec une clé publique à laquelle est associée avec une date d'expiration. Lorsque quelqu'un souhaite accéder à une donnée particulière, il a recours à l'*Ephemerizer* pour jouer le rôle d'oracle de déchiffrement (en effet seul l'Ephemerizer connaît la clé secrète de déchiffrement correspondante), rôle que l'*Ephemerizer* acceptera seulement de jouer si la durée de vie de la donnée n'a pas expiré. Du point de vue de la sécurité, cette architecture est plus faible que celle de *Vanish* car elle possède un point unique de faiblesse, l'*Ephemerizer* lui-même, qui s'il est non-disponible (par exemple suite à une attaque de déni-de-service) empêche complètement le système de fonctionner. L'idée d'avoir une entité centrale qui s'occupe de la gestion des clés afin de permettre une

[274] A. Shamir, « How to share a secret », *in* Communications of the ACM, 1979, vol. 22, pp. 612-613.
[275] R. Perlman, « The Ephemerizer: Making data disappear », Journal of Information System Security (JISSec), 2005, vol. 1, pp. 51-68.

publication éphémère des données a été reprise pour des domaines d'applications très particuliers tels que les réseaux sociaux avec *Xpire!*[276].

Plutôt que de faire disparaître totalement une donnée au bout d'un certain laps de temps, une approche alternative pourrait être de dégrader petit à petit le contenu de cette donnée[277]. Ainsi par exemple, on pourrait imaginer qu'on généralise la valeur d'un attribut comme l'âge en révélant à la place la tranche d'âge ou encore qu'on efface peu à peu des bits de précision servant à décrire la donnée comme dans le cas d'une position géographique où la précision de la localisation gardée en mémoire deviendrait de moins en moins précise jusqu'à éventuellement que cette localisation corresponde à celle de toute la planète. On peut voir l'approche par dégradation de données comme une généralisation de la publication éphémère où au lieu d'être disponible ou non-disponible, la donnée perdrait en qualité au fur et à mesure du temps, de telle manière à ce qu'il reste quand même une certaine utilité à cette donnée.

1.4. Rendre une donnée introuvable

Une des raisons pour lesquelles il est très difficile de mettre en place le droit à l'oubli tient à ce que les moteurs de recherche tels que Google ou encore les agrégateurs de données comme Yasni[278] sont devenus extrêmement compétents à faire remonter toutes sortes de données liées à un individu, même si ses données sont dispersées dans les profondeurs du Web. Cependant de la même manière, on peut considérer qu'une donnée qui existe physiquement mais qui n'est pas indexée par ces mêmes moteurs de recherche (ou alors retournée parmi les derniers résultats) peut être considérée comme ayant été « oubliée » car hors de portée de la plupart des internautes. La décision de la CJUE Google Spain c/ AEPD de mai 2014 va d'ailleurs dans ce sens puisqu'elle semble indiquer que le déréférencement par un moteur de recherche d'une donnée personnelle est une manière légitime d'implémenter le droit à l'oubli.

Ainsi, on peut par exemple rajouter dans le code HTML d'une page web un tag signifiant explicitement aux moteurs de recherche qu'on ne souhaite pas être référencé par ceux-ci. De plus, certaines entreprises de gestion de la réputation numérique (*e-réputation* en anglais) commencent à fleurir depuis quelques années en offrant à leurs clients une aide pour effacer les données qu'ils considèrent comme nocives. Ainsi, ces entreprises proposent de jouer le rôle d'intermédiaire au nom de leur client pour demander à la compagnie hébergeant des données le concernant de les effacer, voir même parfois de noyer ces données sensibles sous des données

[276] J. Backes, M. Backes, M. Dürmuth, S. Gerling & S. Lorenz, « X-pire!: An expiration date for images » in social networks, 2011 (http://arxiv.org/abs/1112.2649).
[277] H. van Heerde, M. Fokkinga, & N. Anciaux, « Balancing privacy and data usability using data degradation », *in* Proceedings of the 12th IEEE International Conference on Computational Services and Engineering (CSE'09), 2009.
[278] http://www.yasni.fr

« positives » qui apparaîtront parmi les premiers résultats renvoyés lorsqu'on tape le nom de ce client dans un moteur de recherche. Il faut noter que, bien souvent, les entreprises d'e-réputation qui se proposent d'aider des individus à « nettoyer leurs données » sont aussi celles qui font de l'agrégation de données, en proposant par exemple de vendre le dossier digital d'un candidat dans le cadre d'une procédure d'embauche. En outre, à ce jour, les approches visant à rendre une donnée introuvable en essayant de tromper les mécanismes de recherche relèvent davantage de l'heuristique et offrent très peu de garanties formelles contrairement aux techniques précédentes dont on peut souvent analyser et prouver les propriétés offertes par une architecture particulière.

1.5. La situation spécifique des réseaux sociaux

Les réflexions actuellement menées sur les aspects juridiques du droit à l'oubli dans des applications web comme les plates-formes de réseaux sociaux ont un pendant informatique, généralement développé dans le cadre plus général de la protection de la vie privée des utilisateurs de ces systèmes. Un des constats possibles, évoqué plus haut et généralement partagé par les informaticiens travaillant sur la protection de la vie privée, est que la position centrale du fournisseur de service lui procure un contrôle total sur les données partagées par les utilisateurs. Étant donné la valeur économique que peut représenter pour eux cette masse d'informations (par exemple lorsqu'elle est organisée de manière à permettre un profilage comportemental à des fins commerciales), le fournisseur de service est souvent considéré comme une source de risque majeure pour la vie privée des utilisateurs. Dans le cas spécifique du droit à l'oubli numérique, lorsqu'un utilisateur demande au service la suppression d'une information – par exemple, une photographie partagée – il peut effectivement observer le fait que cette photographie devient inaccessible pour lui et éventuellement pour d'autres personnes. Par contre, il n'a aucun moyen de s'assurer que ce contenu a réellement été supprimé des serveurs du fournisseur et qu'il n'est pas resté accessible au fournisseur de réseau social. L'affaire « Facebook vs Europe »[279], qui fait suite à l'action de Max Shrems contre Facebook devant la justice irlandaise, a mis en lumière le fait que des éléments cachés aux utilisateurs restaient pour autant conservés sur les serveurs de Facebook. Ainsi, un fournisseur de réseau social qui prendrait soin de ne pas divulguer imprudemment cette information de cette manière pourrait continuer à exploiter des données censées avoir disparu. L'organisation centralisée des réseaux sociaux existants permet cette sorte d'oubli « partiel », entre autres manifestations du contrôle total du fournisseur sur les données qui lui sont confiées. Il ne semble pas y avoir pour

[279] http://europe-v-facebook.org/

l'instant de moyens techniques de vérification ou d'observation efficaces permettant à l'utilisateur d'obtenir une information complète et pertinente sur les traitements effectués et les données conservées par un opérateur distant. En particulier, contrairement aux preuves de récupérabilité qui permettent à un tiers, partie de confiance (par exemple le cloud), de prouver qu'il a bien gardé en sa possession les données confiées par l'utilisateur, il semble techniquement très difficile, voire impossible, de produire une preuve d'effacement qui permettrait au fournisseur de démontrer qu'il a réellement effacé les données d'un utilisateur.

Devant ce constant de relative cécité technique des utilisateurs face à l'application du droit à l'oubli (ou d'autres composantes de leur droit à la vie privée) par un fournisseur de service de réseau social, la communauté de recherche sur la protection de la vie privée en informatique a un point de vue assez consensuel. On estime que distribuer le stockage et les traitements, habituellement entre les mains d'un fournisseur unique, pour le confier à plusieurs entités (possiblement à l'ensemble des utilisateurs), est une évolution de nature à favoriser le contrôle que les individus peuvent espérer avoir sur leurs données.

1.5.1. Distribuer les applications pour un meilleur contrôle par les utilisateurs

L'évolution d'une architecture centralisée vers une architecture distribuée répond à deux besoins fondamentaux. Le premier est l'élimination d'un point de faiblesse unique : si toutes les données sont stockées au même endroit, si une seule entité a le contrôle sur un grand nombre de propriétés (comme la conservation ou la suppression des données, mais aussi la révocation de l'anonymat des utilisateurs ou la protection de leurs communications), alors il suffit d'attaquer cette entité unique pour compromettre l'ensemble du système. Le deuxième besoin auquel répond la distribution est de rapprocher les utilisateurs des données qu'ils publient : si les contenus sont stockés en priorité sur les terminaux des utilisateurs et non sur un service distant, le risque de perte de contrôle au profit d'un tiers est moindre[280]. Le fait de centrer la gestion des données à caractère personnel sur les utilisateurs est d'ailleurs l'un des principes du

[280] S. Riché, G. Brebner et M. Glitter, « Client-side profile storage », NETWORKING Workshops on Web Engineering and Peer-to-Peer Computing, 2002, pp. 127-133.

Privacy by Design et l'un des aspects techniques retenus par la CNIL pour évaluer les risques liés à certains traitements, notamment ceux impliquant des données biométriques[281].

Dans le domaine des réseaux sociaux en particuliers, plusieurs modèles et architectures ont été proposés dans ce sens. Diaspora[282] reste l'exemple le plus célèbre, malgré une révision à la baisse de ses objectifs initiaux. On peut ranger dans la même catégorie des propositions de recherche comme SuperNova[283] et PeerSon[284]. Les trois plates-formes ont en commun de répartir le contrôle sur des serveurs intermédiaires, multiples et possiblement indépendants. Dans ces architectures, l'utilisateur rejoignant le réseau peut choisir le serveur auquel il s'affilie et à qui il décide de faire confiance.

Certaines propositions, comme Safebook[285] ou PrivacyWatch[286], tentent de distribuer complètement ce contrôle en le déportant sur les machines des utilisateurs. Une analyse détaillée montre que dans aucune de ces propositions, la distribution n'est totale pour l'ensemble des fonctionnalités et des propriétés de sécurité[287]. De fait, la distribution de certaines propriétés délicates, comme la non-chaînabilité ou la non-observabilité, semble un problème difficile, auquel toute l'attention nécessaire n'a pas encore été donnée. Néanmoins, si l'on se concentre sur les aspects directement liés à la mise en œuvre du droit à l'oubli (en l'occurrence le stockage et la suppression des données), on constate qu'il existe au moins une proposition de recherche (PrivacyWatch) en présentant un modèle complètement distribué. Dans ce cadre, aucune entité n'a plus de pouvoir qu'une autre pour supprimer ou empêcher la suppression d'une donnée contre la volonté de la personne qui l'a mise en ligne.

Il est donc possible de construire des systèmes de réseaux sociaux dans lesquels les utilisateurs ont un meilleur contrôle sur la suppression des données qu'ils ont mises à disposition, mais de tels systèmes ne sont actuellement disponibles qu'à l'état de démonstrateurs académiques et présentent, indépendamment de cette qualité, des lacunes sur d'autres aspects liés à la sécurité et à la vie privée.

---

[281] M. Moulin et V. Younes-Fellous, « Communication de la CNIL relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données », 2011 (http://www.CNIL.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/Communication-biometrie.pdf). - CNIL, Autorisation unique n° AU-008 - Délibération n°2006-102 du 27 avril 2006 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail, 2006 (http://www.CNIL.fr/documentation/deliberations/deliberation/delib/104/)

[282] https://diasporafoundation.org/

[283] R. Sharma and A.Datta, « SuperNova: Super-Peers Based Architecture for Decentralized Online Social Networks », *in* Fourth International Conference on Communication Systems and Networks (COMSNETS), pp. 1-10, 2012.

[284] S. Doris, A Peer-to-peer Infrastructure for Social Networks, thèse de doctorat, TU Berlin, 2008.

[285] L. Cutillo, R. Molva et T. Strufe, « Safebook: A Privacy-Preserving Online Social Network Leveraging on Real-Life Trust », IEEE Communication Magazine*,* pp. 94-101*,* 2009.

[286] A. T. Ho, *Towards a Privacy-Enhanced Social Networking Site*. Thèse de doctorat, Université de Montréal, 2012.

[287] R. Paiva Melo Marin, G. Piolle et C. Bidan, « An Analysis Grid for Privacy-related Properties of Social Network Systems », *in* ASE/IEEE International Conference on Social Computing (SOCIALCOM 2013), pp. 520--525, Washington D.C., USA, 2013 (IEEE Computer Society, ISBN 978-0-769-5137-1).

1.5.2. Les problématiques spécifiques aux réseaux sociaux distribués

Encore une fois, le contrôle des utilisateurs sur la suppression des données publiées n'est qu'un des aspects qui motivent la conception de plateformes de réseaux sociaux distribuées. Il est également important de noter que ce choix architectural, s'il peut apporter beaucoup en termes de sécurité et de vie privée, implique également certaines difficultés techniques et amène également à effectuer certains compromis.

D'une manière générale, la gestion des politiques de vie privée dans un tel système reste une question ouverte, à laquelle il n'y a peut-être pas de réponse absolue et universelle. En particulier, il n'y a plus de politique de niveau système, imposée par le fournisseur. Cela peut être vu comme une bonne ou une mauvaise chose, mais il s'agit en tous les cas d'une source possible de richesse et de complexité. Chaque utilisateur peut potentiellement concevoir sa propre politique. L'application de ces politiques dans un environnement sans serveur, c'est-à-dire sans point de décision centralisé, est une problématique relativement complexe (notamment dans le cas où les politiques de plusieurs personnes s'appliquent à un même contenu) et qui intéresse vivement certains chercheurs.

D'autre part, les propriétés de vie privée et de sécurité introduites dans ces architectures le sont actuellement avec comme contrepartie des limitations en termes de performances (répartition de la charge de calcul), d'utilisabilité (facilité d'utilisation et de compréhension pour les utilisateurs) et de disponibilité (capacité pour un contenu à pouvoir rester accessible même lorsque l'utilisateur qui le met à disposition est déconnecté).

De plus, ce type d'application complètement distribuée, sans fournisseur de service, remet sur la table la question de l'identification du responsable de traitement. Le problème n'est déjà pas nécessairement simple dans le cas d'école de Facebook, mais en l'absence du fournisseur, la dissociation des différents traitements et des différentes responsabilités entre les utilisateurs de l'application peut s'avérer délicate à traiter pour le juriste.

Enfin, si nombre d'équipes de recherche s'attellent à concevoir le système de réseau social qui sera le plus favorable à la protection des personnes, il faut rester conscient que le problème majeur sera celui de l'adhésion des utilisateurs. En effet, pour qu'un nouveau réseau social puisse trouver sa place dans le paysage existant, il est nécessaire qu'il puisse atteindre une certaine masse critique en termes d'utilisateurs faute de quoi il finira par être délaissé car ses membres n'y trouveront pas leur compte en termes d'interactions sociales. En particulier, il est possible que dans un environnement social et un contexte d'utilisation donné, une seule application puisse survivre, les autres étant condamnées à voir fuir leurs utilisateurs. En France

comme dans une grande partie du monde occidental, l'application généraliste de réseau social est Facebook, et elle n'admet pas vraiment de concurrence. Il faut garder à l'esprit qu'une plate-forme comme Google+ a bénéficié d'investissements considérables de la part de Google, ainsi que d'efforts de toutes natures pour attirer les utilisateurs, voire pour les forcer à s'inscrire (par le biais d'Android ou de Youtube). En dépit de tout cela, l'activité sociale réelle sur cette plate-forme est négligeable. Il est donc probablement illusoire d'espérer que les utilisateurs passeront spontanément d'un réseau où leurs contacts sont tous présents, à un réseau pratiquement désert, même s'il leur propose une excellente protection de leur vie privée ou de leur droit à l'oubli. Si l'on souhaite voir la situation évoluer dans le domaine des réseaux sociaux, on peut envisager que cela passe par une amélioration des plates-formes majoritaires actuelles (mais cela nécessiterait sans doute, pour certaines en tout cas, qu'elles abandonnent leur modèle économique actuel) ou par une interopérabilité réellement efficace entre les systèmes actuels et des systèmes fondés sur des modèles différents. Cette approche, plus pragmatique et probablement plus prometteuse, est celle actuellement choisie par Diaspora, qui permet à ses utilisateurs d'interagir partiellement avec Facebook. Néanmoins, l'efficacité et la richesse de l'interopérabilité technique est elle aussi soumise à la bonne volonté du fournisseur majoritaire, ou à l'efficience d'un type de disposition législative dont on a parfois du mal à observer un effet, même à l'intérieur des frontières de l'Union européenne. Il est possible aussi que l'usage massif de Facebook puisse coexister avec d'autres réseaux sociaux plus ciblés. En effet, nombreux sont les usagers qui sont membres à la fois de Facebook, pour leur vie personnelle et de LinkedIn pour gérer leur carrière professionnelle, ainsi que d'autres réseaux sociaux spécialisés sur une thématique particulière.

La conclusion principale que l'on peut faire du panorama eu égard à la mise en œuvre technique du droit à l'oubli est qu'il semble impossible de proposer une solution générique convenant à toutes les situations mais qu'il faut plutôt développer de manière *ad hoc* une solution répondant à un scénario spécifique dont les hypothèses peuvent être limitatives. Ainsi, les technologies permettant d'envisager un droit à l'oubli efficace sont toujours tributaires d'une architecture applicative qui est plus ou moins contraignante et complexe.

Plusieurs des approches présentées ici sont techniquement séduisantes et laissent espérer la possibilité d'améliorations prometteuses – ce domaine de recherche est d'ailleurs particulièrement actif et la poursuite du projet nous donnera sans doute l'occasion d'y contribuer. Néanmoins, leur analyse renforce notre constat de départ : il semble pour l'instant impossible de concevoir une solution technique parfaitement efficace et totalement générique pour la mise en œuvre absolue d'un droit à l'oubli numérique.

De plus, quand bien même une solution technique générique parfaite existerait, le problème de la confiance que les utilisateurs peuvent avoir ou non dans l'efficacité du système resterait fondamental pour garantir son adoption. Idéalement, on souhaiterait que les propriétés techniques du système puissent être quantifiées et prouvées mathématiquement, d'une manière vérifiable par les outils d'automatisation du raisonnement tels que ceux à l'œuvre dans la conception de systèmes critiques dans des domaines tels que les centrales nucléaires ou encore l'aéronautique. Ainsi, l'expert technique qui connaît le système formel dans lequel la preuve est construite ainsi que les outils de vérification peut, pour lui-même, acquérir une certaine confiance dans la qualité du système. Cependant, il ne lui sera pas forcément possible de propager cette confiance à n'importe quel utilisateur *lambda*. En effet, la preuve peut convaincre l'expert capable de la mettre à l'épreuve, mais l'utilisateur final se retrouve placé en face d'une « épreuve de foi » dans l'expert ou dans le système mathématique qui lui est opposé. Dans cette situation, il reste envisageable que même si on lui présente un système « théoriquement parfait » et « parfaitement implémenté », l'utilisateur ne fasse pas confiance aux capacités et propriétés de ce système. Il est cependant possible de répondre partiellement à cette problématique en jouant la transparence et en essayant d'expliciter de manière claire et pédagogique le fonctionnement du mécanisme technique mettant en pratique le droit à l'oubli.

2. L'EFFECTIVITE JURIDIQUE

Si un droit à l'oubli devait être consacré, il est loisible de comprendre, grâce à l'analyse des moyens techniques d'anonymisation et de disparition des données, que les garanties de mise en œuvre seraient assez limitées. En tout état de cause, d'un point de vue juridique, il ne pourrait pas être absolu et devrait s'articuler avec les droits opposables par les tiers (2.1). Naturellement, son effectivité serait étroitement liée à sa place dans l'échelle des normes (2.2) et aux sanctions dont sa violation pourrait être assortie (2.3).

2.1. L'articulation d'un droit à l'oubli avec les droits opposables par les tiers

« Si l'oubli procédait jadis des faiblesses de la mémoire humaine, de sorte qu'il n'y avait pas à consacrer un droit à l'oubli, la nature y pourvoyant, la société numérique, la libre accessibilité des informations sur Internet, et les capacités sans limites des moteurs de recherche changent considérablement la donne et justifient pleinement qu'un tel droit soit aujourd'hui revendiqué, non comme un privilège qui s'opposerait à la liberté d'information, mais comme un droit humain élémentaire à l'heure de la société de conservation et d'archivage numérique sans limites de toute donnée personnelle et de l'accessibilité immédiate et globalisée à l'information qui caractérisent les technologies contemporaines et la fascinante insouciance qu'elles suscitent »[288]. Si l'on peut convenir de ce nécessaire rééquilibrage, en l'état actuel du droit, il n'est pas possible d'opposer le droit à l'oubli à toutes relations de faits ou diffusion de données personnelles. Néanmoins, le fondement juridique sur lequel il s'adosse conditionne très largement son effectivité face aux droits des tiers.

Lorsque le droit à l'oubli est opposé sur le fondement du droit au respect de la vie privée, il se heurte à des limites conduisant la jurisprudence à refuser, le plus souvent, de le consacrer. C'est le cas notamment en ce qui concerne les fictions du réel ou les dossiers journalistiques se référant à des faits divers ou des affaires judiciaires. Le droit au respect de la vie privée (et plus généralement les droits de la personnalité) et le droit à la protection des données est en effet à concilier avec, d'une part, la liberté d'expression (qui inclut la liberté de création), droit fondamental consacré par l'article 10 de la CEDH et, d'autre part, le droit à l'information.

[288] TGI Paris, Ord. Réf. 25 juin 2009, Vernes c. SAS les Échos, Légipresse, n°266, novembre 2009, p. 215, note N. MALLET-POUJOL.

On constate que le poids de la liberté d'expression face à un droit à l'oubli s'appuyant sur le droit au respect de la vie privée varie selon le domaine dans lequel elle s'exerce. Ainsi, un *distinguo* a été opéré entre la liberté d'expression artistique et la liberté d'expression journalistique, avec une place plus grande pour le droit au respect de la vie privée dans le 1er cas que dans le 2nd [289]. Il en serait sans doute de même si un droit autonome à l'oubli devait être consacré.

Cette approche est en lien étroit avec le droit à l'information du public. Le public a le droit à l'information**.** On peut en déduire, *a contrario*, que si le but de la divulgation n'est pas légitime, la relation de faits ne le sera pas non plus – il s'agit donc là d'une limite. Ainsi, dans certaines situations, le but de la publication pourra légitimer une divulgation. C'est le cas lorsque la publication vise à informer le public. Un élément concernant une personne pourra valablement être diffusé par voie de presse, malgré son absence de consentement, et même contre son consentement, s'il répond à un intérêt d'ordre général, à un besoin d'actualité, voire même s'il satisfait un intérêt culturel. En revanche, si la divulgation d'événements vise le seul agrément du public, elle perd en légitimité car elle ne vise plus l'information du public, elle satisfait une curiosité malsaine et devient inutile.

Ces critères sont transposables à l'activité des moteurs de recherche. Dans le jugement du TGI de Montpellier le 28 octobre 2010, évoqué précédemment, Google avait fait valoir le principe de la liberté d'expression pour se soustraire à l'obligation de désindexation. Les juges énoncent alors que « la liberté d'expression n'étant pas absolue, mais limitée par le droit au respect de la vie privée de chacun, le moyen tiré de la liberté d'expression (…) ne peut être retenu. En effet, le nom patronymique en tant qu'attribut de la personnalité constitue une donnée à caractère personnel, objet d'une protection par le droit au respect de la vie privée, de même valeur normative que la liberté d'expression. La conciliation de ces deux droits fondamentaux s'effectue en recherchant un équilibre entre eux »[290]. Or, on se souvient que dans cette affaire, la plaignante avait demandé la désindexation des pages *web* apparaissant en résultat à la suite de requêtes faites sur la base d'une association de ses nom patronymique et prénom aux termes *swallows* (en anglais *avaler*) et *école de laetitia* qui renvoyait à une série de vidéos pornographiques. « La demande qui se restreint à la désindexation de pages *web* qui apparaissent à la suite de requêtes comprenant le nom patronymique et le prénom de la demanderesse associés à des mots renvoyant à la pornographie n'apporte qu'une restriction à la

[289] I. Paulik, "Liberté d'expression par l'image et respect des droits de la personnalité », obs. sous Cass. 1ère civ. 9 juillet 2003, Petites affiches, 2004, p. 14.
[290] TGI Montpellier, ord. Réf, 28 oct. 2010, Comm. com. électr. n°5, Mai 2011, comm. 47, A. Lepage.

liberté d'expression, restriction justifiée par le droit au respect de la vie privée de Mme Marie C. »[291].

Au regard des motifs mis en avant dans cette affaire, on pourrait penser que, en dehors de l'atteinte à la vie privée, il est difficile d'obtenir gain de cause car l'on buterait sur la liberté d'expression. Il faut bien reconnaître que les avis ne sont pas unanimes et que la mise en balance de la protection des données à caractère personnel et de la liberté d'expression, notamment aux fins de protection de la vie privée ou de l'image divise la doctrine[292]. En réalité, supprimer le site ou la vidéo serait assurément une atteinte au droit à l'information et à la liberté d'expression. Supprimer l'association du nom de la personne à un film ne l'est pas car cette information n'est pas nécessaire à la mise à disposition du film. C'est donc bien d'abord et avant toute chose, le traitement d'une donnée personnelle qui est en jeu.

De fait, l'approche jurisprudentielle retenue dans le cadre de la protection des données personnelles est différente, notamment, à l'égard des moteurs de recherche qui facilitent l'accès aux données.

Dans l'affaire Google Spain c/ AEPD, la CJUE énonce que, dans ce cadre, « il convient notamment d'examiner si la personne concernée a un droit à ce que l'information en question relative à sa personne ne soit plus, au stade actuel, liée à son nom par une liste de résultats affichée à la suite d'une recherche effectuée à partir de son nom, sans pour autant que la constatation d'un tel droit présuppose que l'inclusion de l'information en question dans cette liste cause un préjudice à cette personne. Cette dernière pouvant, eu égard à ses droits fondamentaux au titre des articles 7 et 8 de la Charte, demander que l'information en question ne soit plus mise à la disposition du grand public du fait de son inclusion dans une telle liste de résultats, ces droits prévalent, en principe, non seulement sur l'intérêt économique de l'exploitant du moteur de recherche, mais également sur l'intérêt de ce public à accéder à ladite information lors d'une recherche portant sur le nom de cette personne ».

Il est bien évident toutefois que ce droit ne saurait s'appliquer de manière générale et le juge européen en a bien pris conscience en ajoutant que la prévalence évoquée ci-dessus ne saurait jouer « s'il apparaissait, pour des raisons particulières, telles que le rôle joué par ladite personne dans la vie publique, que l'ingérence dans ses droits fondamentaux est justifiée par

[291] *Ibid.*

[292] Pour un avis favorable à l'application du régime de protection des données, J. Boyer, Droit à l'oubli, droit de suppression, droit de suite : la loi Informatique et libertés doit-elle arbitrer la liberté d'expression ?, Légicom n° 46, 2011/1, p. 77 et s. - Pour un point de vue opposé, J. Frayssinet, "L'articulation de la liberté d'expression avec l'article 7 de la « loi Informatique, fichiers et libertés » en cas de violation de la vie privée n'est pas un fusil à deux coups », RLDI déc. 2009, n° 55, n° 1814, p. 14 et s.

l'intérêt prépondérant dudit public à avoir, du fait de cette inclusion, accès à l'information en question ». C'est donc le fait de « jouer un rôle dans la vie publique » qui peut être pris en compte pour limiter le droit à l'oubli. Selon la CNIL, il y a lieu de considérer que « les hommes politiques, les représentants officiels d'institutions (syndicalistes, religieux, …), les membres de certaines professions réglementées ou les membres de professions appartenant à la sphère médiatique (journalistes, acteurs, chanteurs…) sont naturellement considérés comme ayant un rôle dans la vie publique. A ce titre, il est légitime pour le public d'avoir accès aux informations en lien avec leur rôle public ou activités. A cet égard, un critère pertinent peut être de savoir si l'accès du public à une information particulière participe de sa protection contre des comportements publics ou professionnels contestables (conflits d'intérêts, compétences professionnelles). Par ailleurs, on peut utilement se référer à la notion de « figure publique » pour définir ce qu'on entend par « jouer un rôle dans la vie publique ». Ainsi, une figure publique est une personne qui, en raison de ses fonctions et/ou engagements, a un certain degré d'exposition médiatique ». La CNIL fait néanmoins preuve de prudence en ajoutant que « certaines informations relatives à des personnes publiques relèvent par essence de leur vie privée, comme celles en lien avec leur santé ou leur famille, et n'ont donc pas vocation à apparaître dans les moteurs de recherche. Une distinction doit ainsi être faite entre la nature des informations traitées, même si d'une manière générale le fait qu'elles concernent une personnalité publique milite pour maintenir leur référencement »[293].

La décision de la société Google de procéder sur demande à la désindexation, suivie en cela par d'autres moteurs de recherche, crée néanmoins une situation qui nous semble dangereuse au regard de la liberté d'expression et du droit à l'information[294]. Lorsqu'un usager s'adresse à un responsable de traitement afin d'exercer son droit d'accès, de retrait ou d'opposition, il s'adresse au collecteur de la donnée ou à un sous-traitant. Il fera alors valoir des arguments propres à justifier que le responsable de traitement cesse le traitement. Lorsqu'un usager s'adresse à un fournisseur de service de moteur de recherche, la situation peut paraître plus complexe. Les différentes manifestations auxquelles nous avons participé[295] ont suscité

[293] CNIL, Droit au déréférencement, Les critères communs utilisés pour l'examen des plaintes, http://www.cnil.fr/fileadmin/documents/Vos_libertes/Droit_au_dereferencement-criteres.pdf, point 2.

[294] Rappelons les critiques suscitées par la décision Google Spain c/ AEPD venant des journalistes (à travers Reporters sans frontières) ou de La quadrature du net.

[295] Notamment, M. Boizard, "La tentation de nouveaux droits fondamentaux face à Internet : vers une souveraineté individuelle ? Illustration à travers le droit à l'oubli numérique", Colloque international *Droits et souverainetés à l'âge de l'Internet : quels défis pour l'Europe ?,* organisé par la Chaire européenne Jean Monnet « Union européenne et société de l'Information » de Télécom Bretagne avec le concours de la chaire de Cyberdéfense et Cybersécurité Saint-Cyr / Sogeti / Thales, Rennes 12 septembre 2014. - *Les moteurs de recherche et le droit à l'oubli numérique*, Atelier pour la protection de la vie privée, organisé par INRIA, Cabourg, 16-18 Juin 2014. - *Droit à l'oubli numérique et protection de la vie privée*, Atelier sur la Protection de la Vie Privée (APVP), organisé par INRIA, Les Loges-en-Josas, 17-19 juin 2013.- *Le droit à l'oubli numérique est-il une utopie ?,* Conférence débat, organisé par la Cantine Numérique rennaise, Rennes 21 mai 2013.

des questions, voire des craintes de certains participants quant au pouvoir qu'une telle décision offrait aux moteurs de recherche s'ils s'arrogeaient le droit de procéder sur demande à la désindexation. En effet, le risque est que par le prisme des moteurs de recherche, la réalité de l'information concernant une personne soit tronquée. Une telle approche n'est pas sans inconvénient. Certains estiment par exemple que « le droit à la protection des données personnelles est si peu nuancé et si biaisé en faveur des caprices des individus exerçant (en l'occurrence[296]) des charges publiques qu'il peut être détourné afin de faire taire les activités relevant de la liberté de critique sur Internet »[297].

En laissant au fournisseur de moteur de recherche l'entière décision de supprimer ou non un lien vers un contenu, on présuppose qu'il puisse apprécier le traitement de données fait par un tiers, ce qui peut s'avérer extrêmement dangereux. De telles procédures, « si elles étaient exigées par la Cour, conduiraient vraisemblablement soit au retrait automatique de liens vers tout contenu faisant l'objet d'une opposition, soit à un nombre ingérable de demandes traitées par les fournisseurs de services de moteur de recherche sur Internet les plus populaires et importants »[298]. Des procédures de retrait existent bien mais elles portent sur des contenus illicites[299], alors que l'affaire évoquée concernait une demande tendant à faire supprimer des liens permettant d'accéder à des informations légales et légitimes qui sont entrées dans la sphère publique. Ainsi, comment un fournisseur international de moteur de recherche peut-il traiter une demande de déréférencement vers un article de presse qui évoque le comportement sulfureux d'une personne connue dans un pays donné ? On discerne immédiatement le danger d'une telle prérogative. Ainsi, un article posté en 2007 par un journaliste économique de la BBC sur son blog, relatant la démission forcée de Stan O'Neal, ancien patron de la banque d'affaires américaine Merrill Lynch, a été effacé de certaines recherches[300]. Pareille initiative n'est évidemment pas conforme à la décision Google Spain c/ AEPD qui conditionne assez strictement l'exercice du déréférencement mais si la décision est laissée à l'arbitrage du moteur de recherche, il y a fort à parier que ces cas se multiplieront. Il est donc indispensable de soumettre ces déréférencements au contrôle d'une autorité indépendante. La CNIL envisage cette hypothèse et érige la source journalistique en critère d'appréciation du déréférencement. Elle estime, expliquant le 11ème critère qu'elle a défini que : « Le fait que la diffusion d'une information s'effectue par un organe de presse est à prendre en considération et peut peser dans

[296] Il s'agissait d'une critique illustrée par l'arrêt de la Cour d'appel de Bourges du 11 janvier 2007 qui, sur le fondement de l'article 38 de la loi de 1978, avant ordonné le retrait d'une liste noire de notaires du site d'une association.
[297] P. Trudel, "Quelles limites à la googleisation des personnes" ? *in La sécurité de l'individu numérisé, Réflexions prospectives et internationales*, S. Lacour (dir.), L'Harmattan 2010, p.53.
[298] Aff. C-131/12, concl. Avocat général Niilo Jääskinen, § 133. Arrêt SABAM du 16 février 2012, aff. C-360/10, point 48.
[299] Directive 2000/31 sur le commerce électronique.
[300] http://www.lesechos.fr/04/07/2014/lesechos.fr/0203619163952_droit-a-l-oubli---google-fait-disparaitre-des-articles-de-presse.htm?texte=#vhtXHyQRJFz4zbJ8.99.

l'appréciation qui sera faite d'une demande de déréférencement. Toutefois, cela ne saurait conduire de manière systématique à refuser un déréférencement. Ce critère doit être combiné avec d'autres, par exemple celui de la durée de la diffusion ou du préjudice pour la personne concernée ». On le voit, c'est une appréciation toute en nuance qui est ici recommandée[301].

Un retour sur la mission des hébergeurs permet de comprendre les difficultés de mise en œuvre du déréférencement. L'une des différences essentielles entre la mission légale de l'hébergeur et la mission potentielle du moteur de recherche tient à ce que le premier n'engage sa responsabilité que dans l'hypothèse où le contenu est illicite. L'étape préalable à toute action de sa part est donc la caractérisation de l'illicéité du contenu. Ainsi, en vertu des articles 6, I, 2 et 6, I, 3 de la loi n° 2004-575 du 21 juin 2004, les fournisseurs d'hébergement ne peuvent pas voir leur responsabilité civile ou pénale engagée à raison des informations stockées à la demande d'un destinataire de ces services s'ils n'avaient pas effectivement connaissance de l'activité ou de l'information illicites ou si, dès le moment où ils en ont eu connaissance, ils ont agi promptement pour retirer ces informations ou en rendre l'accès impossible.

Initialement, la directive 31/2000 avait été interprétée et transposée de manière beaucoup plus restrictive. L'article 43-8 de la loi n° 86-1067 du 30 septembre 1986, posait un principe d'irresponsabilité pénale et civile des fournisseurs d'hébergement. Ce principe d'irresponsabilité n'avait cependant pas vocation à jouer si, ayant été saisis par une autorité judiciaire, les fournisseurs n'agissaient pas promptement pour empêcher l'accès à ce contenu. Ainsi, à l'instar de la directive communautaire, la loi française dispensait l'hébergeur de toute obligation générale de surveillance puisque sa responsabilité devait être appréciée au regard de sa promptitude à réagir aux injonctions d'une autorité judiciaire, sans qu'il ait eu, au préalable, à faire preuve de diligence en vue de déceler l'existence d'un site au contenu illicite.

La disposition offrait une position relativement confortable à l'hébergeur dont la situation pouvait, dans certaines hypothèses, s'avérer délicate. En effet, en prenant l'initiative de ne pas diffuser une information parce qu'il pense que son contenu contrevient à une disposition légale ou réglementaire et, qu'ultérieurement, il s'avère qu'il n'en était rien, il risque de voir sa responsabilité contractuelle engagée vis-à-vis de l'auteur du message[302]. La disposition évitait donc au fournisseur d'avoir à supporter les conséquences préjudiciables d'une décision parfois difficile à prendre, de censurer une information dont il soupçonne le caractère illicite puisque, *a priori*, sa responsabilité était limitée au cas où il n'a pas réagi à la saisine de l'autorité judiciaire.

---

[301] CNIL, Droit au déréférencement, Les critères communs utilisés pour l'examen des plaintes, http://www.cnil.fr/fileadmin/documents/Vos_libertes/Droit_au_dereferencement-criteres.pdf.

[302] Voir, en ce sens, V. Sédaillan, *Droit de l'Internet : réglementation, responsabilités*, *contrats*, éd. Net Press, 1997, p. 128.

La règlementation actuelle comporte une solution médiane. Le caractère illicite peut être dénoncé par toute personne et c'est sur cette base que l'hébergeur doit agir. Néanmoins, afin d'éviter les risques de délation abusive, l'article 6, I, 4 prévoit que toute personne qui dénoncerait aux intermédiaires le caractère illicite d'un contenu afin d'en obtenir le retrait ou d'en faire cesser la diffusion s'expose à une peine d'un an d'emprisonnement et de 15 000 euros d'amende dès lors qu'elle sait pertinemment que cette information est inexacte.

Si la mission de l'hébergeur est délicate, elle reste strictement encadrée. Il n'en va pas de même du fournisseur de service de moteur de recherche qui est amené à apprécier la légitimité d'une demande de désindexation aux contenus tant licites qu'illicites.

Certains regrettent l'absence de principe de subsidiarité qui consisterait à obliger les victimes à s'adresser d'abord à l'éditeur du site puis, dans un second temps seulement, au moteur de recherche. Ne pas imposer ce principe « contribue à déresponsabiliser les éditeurs de site, alors qu'ils devraient être en première ligne »[303]. La remarque nous semble juste si le principe vise à faciliter l'appréciation du contenu licite ou illicite par l'éditeur du site. Il s'agirait également, à notre sens, d'éviter des désindexations abusives, contraires à l'intérêt public. Il conviendrait alors de considérer que si l'éditeur du site adresse un refus motivé de retrait du contenu qu'il estime licite, alors il serait possible de passer par le moteur de recherche afin de limiter l'accès à l'information parce qu'elle n'est pas ou plus pertinente pour le public mais, à notre sens, avec l'avis d'une autorité indépendante telle que la CNIL. Si le contenu est illicite, c'est la responsabilité de l'hébergeur qui devrait être engagée à défaut de prompte réaction[304]. Ajoutons que, d'un point de vue économique, Google est un fournisseur à dimension internationale. Il est sans doute excessif de faire supporter le coût financier du traitement des demandes de déréférencement par des fournisseurs de taille modeste dont le poids financier est très en deçà de celui d'un géant comme Google. A tout le moins, ce serait hypothéquer la survie de certains fournisseurs.

---

[303] L. Marino, "Un « droit à l'oubli » numérique consacré par la CJUE », JCP G 2014, p. 768.

[304] Sur le site de la CNIL il est désormais indiqué : « Pour faire supprimer d'un moteur de recherche une page comportant des informations vous concernant, vous disposez de deux solutions différentes, depuis l'arrêt de la Cour de Justice de l'Union européenne (CJUE) du 13 mai 2014 :

Vous pouvez demander la suppression de ces informations au site d'origine;

Vous pouvez demander à ce que ces informations ne soient plus indexées par les moteurs de recherche.

Ces deux démarches sont indépendantes l'une de l'autre. Nous vous invitons à privilégier la première, ou à les effectuer en parallèle. En effet, ce nouveau « droit au déréférencement » permet seulement la suppression d'un ou de plusieurs résultat(s) de recherche (liens) vous concernant, à partir d'une recherche sur votre nom. Toutefois, les informations restent accessibles sur le site d'origine, que ce soit à partir d'autres requêtes que celles de votre nom, ou par le biais d'autres moteurs de recherche auxquels vous ne vous êtes pas adressé », http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/comment-effacer-des-informations-me-concernant-sur-un-moteur-de-recherche/.

La CNIL propose désormais une liste de critères permettant d'apprécier les demandes de déréférencement, liste qui n'est pas exhaustive[305]. Elle est présentée sous forme de 13 questions dont le contenu est ensuite explicité :

« 1. Les résultats de recherche sont-ils relatifs à une personne physique ? Le résultat apparait-il à la suite d'une recherche effectuée à partir du nom de la personne concernée ?

2. S'agit-il d'une personne publique ? Le plaignant joue-t-il un rôle dans la vie publique ?

3. Le plaignant est-il mineur ?

4. Les données sont-elles exactes ?

5. Les données sont-elles pertinentes et/ou excessives ?

A. Les données sont-elles relatives à la vie professionnelle du plaignant?

B. L'information est-elle potentiellement constitutive de diffamation, d'injure, de calomnie ou d'infractions similaires à l'encontre du plaignant ?

C. L'information reflète-t-elle une opinion personnelle ou s'agit-il d'un fait vérifié ?

6. L'information est-elle sensible au sens de l'article 8 de la Directive 95/46/CE ?

7. L'information est-elle à jour ? L'information a-t-elle été rendue disponible plus longtemps que nécessaire pour le traitement ?

8. Le traitement de l'information cause-t-il un préjudice au plaignant ? Les données ont-elles un impact négatif disproportionné sur la vie privée du plaignant ?

9. Les informations issues du moteur de recherche créent-elles un risque pour le plaignant ?

10. Dans quel contexte l'information a-t-elle été publiée ?

A. Le contenu a-t-il volontairement été rendu public par le plaignant ?

B. Le contenu devait-il être public ? Le plaignant pouvait-il raisonnablement savoir que le contenu serait rendu public ?

11. Le contenu a-t-il été rendu public à des fins journalistiques ?

12. La publication de l'information répond-elle à une obligation légale ? L'auteur de la publication avait-il l'obligation de rendre cette donnée personnelle publique ?

13. L'information est-elle relative à une infraction pénale ? »

L'influence de la décision Google Spain contre l'AEPD est évidente. Pour l'essentiel, les critères renvoient aux différents points d'alerte que nous avons déjà soulignés. Malgré cette

[305] CNIL, Droit au déréférencement, Les critères communs utilisés pour l'examen des plaintes, http://www.cnil.fr/fileadmin/documents/Vos_libertes/Droit_au_dereferencement-criteres.pdf.

liste, la marge de manœuvre reste large pour les fournisseurs de moteurs de recherche et ne fournit pas toutes les garanties permettant d'éviter les dérives.

Une autre difficulté de mise en œuvre du droit à l'oubli *via* la désindexation ou l'effacement réside dans la détermination du délai à partir duquel la demande peut être formulée. Nous l'avons indiqué, le temps est traditionnellement considéré comme une composante du droit à l'oubli. Il est vrai néanmoins que la société du numérique accélère le rythme de nos vies et impacte nécessairement la donnée temporelle. Dans l'affaire Google Spain contre AEPD, la Cour de justice de l'Union fait de l'écoulement du temps un paramètre parmi d'autres d'appréciation du droit à l'oubli. Il permet de caractériser la perte de pertinence de l'information. Ce n'est pas, toutefois, le seul critère. La qualité de la personne concernée est également un critère de reconnaissance du droit à l'oubli. Mais précisément, *quid* des informations concernant, au moment de la demande de retrait, un illustre inconnu mais devenant ultérieurement un personnage public (politique par exemple) ?

En raisonnant au regard du dispositif de protection des données à caractère personnel, on peut considérer que lorsque le traitement d'une donnée est initialement légitimé par le consentement de la personne concernée, on ne voit pas très bien pourquoi une demande de désindexation ou d'effacement serait enfermée dans un quelconque délai. En revanche, lorsque la licéité du traitement tient à une autre cause légale (prévue par les articles 6 ou 7 de la loi informatique et libertés), il en va tout autrement. D'autres contraintes viennent alors conditionner la demande de la personne concernée comme nous l'avons expliqué au sujet des données transmises aux fournisseurs de SRS notamment. Ainsi, certains textes prévoient des durées de conservation spécifiques qui s'imposent à la personne concernée. De la même manière, il a déjà été noté que la portée du droit à l'effacement est limitée par le fait que dans certains cas, une limitation du traitement peut se substituer à l'effacement.

Mais c'est surtout la vocation du droit à l'effacement à être limité par la nécessité de conserver les données qui reste le sujet le plus sensible. Le droit à l'effacement cède en effet lorsque paraît le devoir de mémoire ou, plus simplement, de conservation. Cette question de l'équilibre des droits est certainement une des plus importantes car si certains craignent que le droit à l'effacement ne l'emporte sur d'autres droits, on peut aussi craindre la situation inverse, laquelle conduirait à une réduction considérable du droit à l'effacement. Ainsi, nous l'avons indiqué tout au long des développements, l'article 17 de la proposition de règlement sur la protection des données à caractère personnel prévoit, dans un paragraphe 3, une série d'exceptions dont l'interprétation demeure délicate. Plusieurs hypothèses de rétention légitime

des données renvoient à des situations particulières de traitements envisagées par le chapitre 9 du règlement.

Il s'agit tout d'abord de l'exercice de la liberté d'expression. Sont visées les exemptions et dérogations prévues par les Etats membres aux seuls fins de journalisme ou d'expression artistique ou littéraire. Cette exception a rassuré les entreprises de presse qui craignaient que le renforcement du droit à l'oubli ne remette en cause la liberté d'expression. Internet, en tant que mode d'expression d'idées et d'informations, doit à ce titre être protégé, d'autant plus qu'il semble particulièrement adapté pour permettre la réalisation complète des potentialités garanties par l'article 10 de la Convention européenne des droit de l'homme[306]. Les autres exceptions concernent la santé publique, conformément à l'article 81, les finalités de recherche historique, statistique et scientifique, conformément à l'article 83, le respect d'une obligation légale de conserver les données à caractère personnel prévue par le droit de l'Union ou par la législation d'un État membre à laquelle le responsable du traitement est soumis; la législation de l'État membre doit répondre à un objectif d'intérêt général, respecter le contenu essentiel du droit à la protection des données à caractère personnel et être proportionnée à l'objectif légitime poursuivi. Notre objet n'est pas de les commenter, mais de mettre en évidence la logique critiquable qui préside à cette construction faite d'un droit et d'exceptions. Le régime de l'exception ne nous semble pas satisfaisant car il introduit une hiérarchisation entre les objectifs. C'est peut-être une occasion de regretter la disparition du terme de droit à l'oubli, terme qui se situe dans un même champ sémantique que celui de mémoire.

Enfin, et pour conclure, on peut se demander si le balancement entre droit et exceptions ne méconnaît pas la nature même des dispositifs numériques qui sont des dispositifs de mémoire, comme cela a été souligné dans l'analyse des moyens techniques et est clairement démontré dans les analyses, notamment sociologiques, qui montrent tout l'intérêt de la construction de traces, notamment dans une perspective de renforcement de la confiance.

2.2. La place d'un droit à l'oubli dans l'échelle des normes

La place du droit à l'oubli dans l'échelle des normes est fondamentale dans la mesure où la diffusion des informations sur la toile, par définition, ne connaît pas de frontières géographiques. Le droit à l'oubli circonscrit au territoire national aurait incontestablement une effectivité limitée. Néanmoins, la perception des atteintes au droit des personnes peut différer

[306] S. Turgis, « La coexistence d'Internet et des médias traditionnels sous l'angle de la Convention européenne des droits de l'homme », RTDH, 2013, n° 93.

d'un pays à l'autre. Aux Etats-Unis par exemple, les lois antiterroristes imposent aux compagnies aériennes de divulguer les informations les plus diverses sur leurs passagers, permettant la réalisation de fichiers aux données précises, ce qui heurte certaines législations européennes. Cette disparité favorise l'impunité. Il est ainsi très aisé d'implanter son siège social dans un pays peu regardant pour se mettre à l'abri d'actions judiciaires tendant à obtenir la suppression d'une donnée privée.

C'est très certainement ce qui explique qu'après avoir légiféré par voie de directive, en 1995, les instances européennes aient préféré opter pour la voie règlementaire, plus stricte d'application. Pour autant, en marge du processus législatif, des initiatives tendent à privilégier la *soft law* en élaborant des chartes de bonne conduite.

2.2.1. Le choix d'un règlement européen

La mise en œuvre d'un règlement constitue un avantage pour les entreprises et pour les usagers, en ce qu'il impose un ensemble de règles uniques en matière de protection des données personnelles, ce qui constitue une source de sécurité juridique et, subséquemment, une plus-value indéniable pour les entreprises européennes[307]. Outre les effets positifs qu'engendrerait l'adoption d'un règlement, les mesures que contient la proposition conduiraient à une réduction des formalités administratives pesant sur les responsables de traitement.

2.2.1.1. Les avantages d'un règlement pour les responsables de traitement

Le choix d'un règlement, comme instrument juridique destiné à moderniser et renforcer la protection des données personnelles au sein de l'Union européenne, permet de procurer une plus grande sécurité juridique et un avantage concurrentiel aux entreprises.

2.2.1.1.1. Une source de sécurité

Dans le cadre de la transposition d'une directive, les États membres disposent d'une marge de manœuvre leur permettant de maintenir ou d'introduire des régimes particuliers pour des situations nationales spécifiques. Cette souplesse, conjuguée à une transposition parfois non fidèle de la directive par les Etats membres, peut générer une disparité des législations nationales applicables sur le territoire de l'Union. Or, ces différences sont de nature à contrarier l'un des principaux objectifs de la directive 95/46 d'assurer la libre circulation des données à

[307] Voir F. Bencheliha, *La réforme européenne de la protection des données personnelles et de la vie privée*, mémoire 2013 (dir.) Annie Blandin.

caractère personnel dans le marché intérieur. Les responsables de traitement sont parfois dans l'obligation de composer avec vingt-huit législations nationales sensiblement différentes. Cette absence d'harmonisation de l'environnement juridique conduit à une insécurité juridique tant pour les responsables de traitement que pour les personnes concernées. Ce constat s'est confirmé à l'issue des consultations publiques et études du cadre juridique actuel lancées par la Commission européenne[308] qui soulignaient la nécessité de renforcer la sécurité juridique et d'assurer des conditions égales aux responsables du traitement[309].

La Commission a donc décidé d'adopter un nouveau cadre juridique par la voie, cette fois-ci, d'un règlement. La particularité du règlement, est de créer un droit applicable immédiatement[310] et uniformément dans l'ensemble de l'Union sans qu'il soit nécessaire pour les États membres d'adopter une loi nationale de transposition. Ce règlement permettra aux entreprises de disposer de règles claires et uniformes, source de sécurité juridique et d'allègement des charges administratives.

2.2.1.1.2. Un avantage concurrentiel pour les entreprises européennes

La protection des données personnelles doit s'imposer à l'économie de marché. La difficulté de légiférer dans ce domaine réside dans les différents intérêts en présence. Il est nécessaire que les données personnelles puissent bénéficier d'une protection sans toutefois que celle-ci « ne détende les ressorts des stratégies gagnantes de l'entreprise, notamment sa capacité d'innovation et d'adaptation rapide »[311]. Par le biais de la proposition de règlement, l'Union européenne souhaite garantir un niveau élevé de protection des données et permettre aux entreprises européennes de tirer profit de l'économie numérique.

Dans une certaine mesure des règles uniformes, adaptées aux évolutions technologiques et applicables dans l'ensemble de l'Union européenne peuvent constituer un avantage concurrentiel pour les entreprises responsables de traitement.

D'une part, de manière générale, un règlement permettra de supprimer les obstacles à l'entrée sur le marché découlant d'un manque d'harmonisation entre les régimes juridiques des Etats membres. Ce serait une avancée majeure, notamment, pour les petites et moyennes entreprises qui voient dans les différences de régime, des coûts générant un frein au développement de leurs activités en dehors du territoire national. En outre, l'allègement des

---

[308] Voir les réponses à la consultation publique organisée par la Commission : http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0003_en.htm.

[309] COM(2010) 609 final, *Une approche globale de la protection des données à caractère personnel dans l'Union européenne*, p.4.

[310] Art. 288 TFUE.

[311] P. de Woot, « Stratégies des entreprises et données personnelles » *in La protection de la vie privée dans la société de l'information*, sous la direction de P.Tabatoni, Paris, PUF pp.101-219

charges administratives pourrait, selon la Commission européenne, permettre aux entreprises européennes de réaliser une économie substantielle chiffrée (par la Commission européenne) à environ 2,3 milliards d'euros par an.

D'autre part, l'uniformisation est de nature à renforcer la confiance des consommateurs dans les différents services en ligne. Il est bien évident que la confiance des consommateurs est de nature à accroître le flux des échanges de biens et de services sur Internet. De cette façon, les entreprises du secteur seront en mesure d'augmenter leur offre et d'innover afin de répondre à la demande des consommateurs. Dans ce schéma idéal, la compétitivité des entreprises en sera renforcée et la création d'emplois augmentée.

Cette confiance peut s'étendre aux consommateurs non-européens qui peuvent voir dans ce cadre juridique l'assurance que leurs données personnelles seront traitées avec précaution et bénéficieront d'une protection élevée. Les entreprises européennes, disposeront ainsi d'un avantage concurrentiel à l'échelle mondiale qui leur permettra de faire face à la concurrence des entreprises non-européennes et notamment américaines, qui bénéficient d'un cadre juridique plus souple basé sur l'autorégulation.

2.2.1.2. La place d'un droit à l'oubli dans un règlement

Les développements consacrés aux contours du droit à l'oubli nous permettent d'affirmer qu'il serait cohérent de placer le droit à l'oubli dans un dispositif de protection des données personnelles. La très large acception du concept de données à caractère personnel nous y incite tout particulièrement. La place qui lui avait été attribuée dans la première mouture de la proposition de règlement européen n'était sans doute pas idéale compte tenu, notamment, du contenu de l'article dont il constituait l'intitulé (article 17 de la proposition de règlement) qui laissait à croire que l'oubli passait obligatoirement par l'effacement de la donnée. Or, le droit à l'oubli n'est pas réductible à un droit à l'effacement d'une donnée.

Il nous semble possible à ce stade de songer à deux propositions. On pourrait envisager soit, une disposition à part, propre au droit à l'oubli et embrassant un traitement qui serait considéré comme illicite parce qu'il porte une atteinte excessive au droit à la tranquillité de la personne, soit une disposition générale introductive qui érigerait le droit à l'oubli au rang des fondements de la protection des données à caractère personnel.

Cette seconde proposition a notre préférence. La jurisprudence rendue et les aménagements dont le droit de la protection des données doit faire l'objet laissent à penser que le droit à l'oubli est implicitement l'un des fondements des prérogatives reconnues aux

personnes concernées par des traitements de données. Le rendre explicite conforterait les individus dans le respect de leurs droits.

2.2.1.3. L'application du règlement dans l'espace.

La problématique de l'application territoriale du dispositif est résolue différemment selon qu'il s'agit d'une directive ou d'un règlement. Dans le cadre d'une directive, la loi applicable sera la loi nationale prise pour transposer la directive. Le traitement répréhensible ne sera poursuivi que sur le territoire de l'Etat où il est effectué. S'agissant d'un réseau social comme Facebook, réseau social à finalité personnelle le plus fréquenté au monde, les actions qui seront engagées échoueront généralement sur le fait que le fournisseur est établi aux Etats-Unis. Certes, Facebook adhère aux programmes « *Safe Harbor framework* » établis entre le Département américain du Commerce et l'Union européenne, ainsi qu'entre le Département américain du Commerce et la Suisse pour la collecte, l'utilisation et l'enregistrement des données provenant de l'Union européenne[312]. Un certain nombre de liens et d'informations peuvent être mis en place pour les utilisateurs n'étant pas de la nationalité ou ne résidant pas dans le pays de la loi appliquée. Tel est le cas pour les membres de Facebook qui sont situés en dehors des Etats-Unis et du Canada.

S'agissant de Google, la situation est différente car le mode organisationnel est déconcentré si bien qu'il sera parfois possible de poursuite l'établissement local au sein duquel sont réalisées les opérations de traitement. Il résulte du considérant 19 de la directive 95/46 que « l'établissement sur le territoire d'un État membre suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable ». La CJUE s'est prononcée sur la responsabilité de Google dans l'affaire Google Spain c/ AEPD[313]. Google estimait que le traitement de données à caractère personnel qui était mis en cause dans cette affaire est effectué exclusivement par Google Inc. qui exploite Google Search sans aucune intervention de la part de Google Spain, l'activité de ce dernier se limitant à la fourniture d'un soutien à l'activité publicitaire du groupe Google qui est distincte de son service de moteur de recherche (pt 51). Néanmoins, à s'en tenir à une interprétation littérale de l'article 4 §1 a) de la directive, le traitement de données à caractère personnel n'a pas à être effectué *par* l'établissement concerné lui-même. Il doit l'être *dans le cadre des activités* de celui-ci. Or, l'activité de l'établissement local consistant à assurer la promotion et la vente des espaces publicitaires proposés par le moteur de recherche pour rentabiliser le service proposé par ce fournisseur, il agit bien dans le cadre des activités de ce

[312] Politique de confidentialité Facebook, partie « Autres informations dont vous devez avoir connaissance ».
[313] Aff. C131/12 préc..

dernier. Il s'agit d'activités indissociablement liées, l'activité de l'établissement ne se justifiant que par l'existence du moteur de recherche dont elle est destinée à assurer la rentabilité économique.

La proposition de règlement amendée aborde frontalement la question de l'application territoriale du dispositif de protection. L'article 3 prévoit une application uniforme au traitement des données à caractère personnel effectué *dans le cadre des activités d'un établissement* d'un responsable du traitement de données ou d'un sous-traitant sur tout le territoire de l'Union Européenne, *que le traitement ait lieu ou pas dans l'Union.*

Il précise également qu'il s'applique au traitement des données à caractère personnel appartenant à des personnes concernées dans l'Union (= ressortissant de l'UE ? la version antérieure visait les personnes ayant leur résidence sur le territoire) par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes concernées; ou à l'observation de ces personnes concernées. La commission LIBE a préféré cette formule à « l'observation de leurs comportements » estimant que le texte « devrait couvrir non seulement l'observation du comportement des résidents de l'Union par tout responsable du traitement qui n'est pas établi dans l'Union, notamment par le traçage sur Internet, mais aussi la collecte et le traitement des données à caractère personnel des résidents de l'Union ».

Le présent règlement s'appliquerait aussi, selon l'article 3 §3, au traitement de données à caractère personnel par un responsable du traitement qui n'est pas établi dans l'Union, mais dans un lieu où la législation nationale d'un État membre s'applique en vertu du droit international public.

Enfin, précisons que le G29, chargé d'établir des lignes directrices précisant la façon dont les moteurs de recherche doivent appliquer le déréférencement, a estimé que le droit à la protection des données ne doit plus seulement concerner les déclinaisons nationales de Google. Alors qu'auparavant le dispositif s'appliquait aux sites « locaux » comme Google.fr, Google.co.uk, Google.de ou Google.it, le groupe recommande de l'élargir désormais à Google.com. Il considère que : « Limiter le retrait de ces liens aux domaines européens, en partant du principe que les utilisateurs tendent à utiliser les moteurs de recherche sur leurs domaines nationaux ne peut pas être considéré comme un moyen suffisant de garantir de façon

satisfaisante les droits relatifs aux données individuelles »[314]. Le rapport du Comité consultatif de Google est évidemment contre cette position et estime que le droit à l'oubli devrait être limité aux seules versions européennes du moteur de recherche[315].

2.2.2. La charte : un outil d'implication des acteurs économiques

L'effectivité du droit à l'oubli peut naturellement être améliorée par l'implication des acteurs du marché à travers la réalisation de chartes ou de codes de bonne conduite par lesquels ils prendraient un certain nombre d'engagements permettant d'agir préventivement[316]. C'est une des voies choisie par la France puisqu'elle s'est dotée d'une Charte du droit à l'oubli dans les sites collaboratifs et les moteurs de recherche. Les codes de bonne conduite ont néanmoins leurs limites[317] et ne privent pas d'une réflexion sur l'adoption de sanctions adéquates.

Le XX^{e} siècle a vu fleurir les codes de bonne conduite, parfois appelés charte ou *guidelines*. Un code de conduite peut être public ou privé. Il sera public, s'il est adopté par une autorité publique. Il sera privé, s'il émane de partenaires privés. C'est aux Etats-Unis, dans les années 30, qu'apparaissent les premiers codes de conduite privés[318]. On en dénombre aujourd'hui une grande variété. Les secteurs de l'activité économique concernés par ce type de démarche volontaire sont extrêmement divers. A titre d'exemple, en 2000, on dénombrait 145 codes de conduite touchant à la gestion de l'environnement[319], 148 sur les conditions de travail et 117 sur la protection du consommateur[320].

La portée territoriale de ces codes est elle-même très variable. Ils peuvent se cantonner à une entreprise[321] ou aux frontières d'un Etat mais ils ont le plus souvent une portée

---

[314] Guidelines on the implementation of the court of justice of the european union judgment on "Google Spain and inc v. Agencia española de protección de datos (AEPD) and Mario Costeja González", 26 novembre 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf et C-131/12http://www.cnil.fr
/linstitution/actualite/article/article/communique-g29-droit-au-dereferencement-le-g29-adopte-des-lignes-directrices/

[315] The advisory council to Google on the right to be forgotten, 6 février 2015,
https://drive.google.com/file/d/0B1UgZshetMd4cEI3SjlvV0hNbDA/view?pli=1

[316] Charte du 13 oct. 2010 sous l'égide de N. Kosciusko-Morizet, alors Secrétaire d'Etat à l'économie numérique.

[317] V. notamment M. Boizard, « Les codes de conduite privés, un instrument volontaire juridiquement efficace ? » *in Les approches volontaires et le droit de l'environnement, actes du colloque*, sous la direction de N. Hervé-Fournereau, Préface de Stavos Dimas, PUR 2008, p. 147 s..

[318] Notamment, le Code éthique professionnel établi pour les conseils en organisation et le Code de la publicité en 1937.

[319] Ainsi par exemple, la Charte des entreprises pour un développement durable institué en 1991 à l'initiative de la Chambre de commerce internationale a une portée très large. On peut également citer le Code international de conduite pour la distribution et l'utilisation des pesticides, ONU pour l'alimentation et l'agriculture, Version adoptée lors de la 13ème session du Conseil de la FAO en novembre 2002.

[320] Source OCDE, *Les codes de conduite des entreprises – Etude approfondie de leur contenu*, Paris, OCDE, 2000. On doit également faire état d'un secteur émergeant, celui d'Internet, V. par ex., X. Linant de Bellefonds, « Les hyperliens », Communication – Commerce électronique 2003, n°5, repères p. 3.

[321] On peut ainsi évoquer le cas de la société IBM qui, en 1984, s'est dotée d'une charte intitulée « règle de conduite dans les affaires ».

européenne, voire internationale. Ils acquièrent, dans ce dernier cas, une force supplémentaire parce qu'ils s'adressent alors à des professionnels appartenant au secteur d'activité visé par le code sans qu'une adhésion individuelle soit nécessaire. En droit international, les premiers codes de conduite discutés touchent les transferts de technologie et les sociétés transnationales[322].

Comment définir un code de conduite ? Un code de conduite, c'est un ensemble de recommandations qui sont, au sens juridique du terme, dépourvues de caractère obligatoire pour ceux auxquels elles s'adressent et qui sont susceptibles d'évoluer en fonction des circonstances[323].

Pour le Conseil économique et social des Nations Unis : « Le but de tout code de conduite est de réglementer la conduite des entités auxquelles il s'applique. La réglementation pourra être plus ou moins rigoureuse, selon les objectifs particuliers recherchés, et selon que ses auteurs seront ou non disposés à promulguer des règles spécifiques plutôt que des directives générales et à faire un effort résolu pour appliquer ces règles quel que soit leur caractère juridique officiel »[324].

Les codes de conduite n'ont pas, en principe, vocation à se substituer à la réglementation légale applicable[325]. Ils intègrent le plus souvent les règles légales pertinentes. Naturellement, certains codes vont au-delà, et créent des règles supplémentaires.

Les motivations des professionnels qui élaborent un code de conduite sont multiples. On peut toutefois considérer, d'une manière générale, que l'adoption de tels codes est dictée par le souci d'éviter une réglementation trop lourde, trop contraignante, voire inadaptées aux besoins de la profession[326].

Cela ne signifie pas qu'un code reproduisant des obligations légales est dépourvu d'intérêt pour ses destinataires. L'avantage provient de ce que s'inscrivant dans une démarche volontariste, les entreprises donnent au public, autrement dit aux clients potentiels, une

[322] Les négociations du code de conduite ont commencé en 1976 et le code n'a jamais abouti.
[323] Cette définition fait référence aux critères proposés pour les codes relatifs aux sociétés transnationales et aux transferts de technologie par le « Groupe de personnalités de l'ONU », Doc. ONU E/5500, p. 62 cité par G. Farjat, « Réflexions sur les codes de conduite privés », *in le Droit des relations économiques internationales*, Etudes offertes à B. Goldman, Litec 1982, p. 48.
[324] Conseil économique et social des Nations Unies, « Sociétés transnationales : l'élaboration d'un code de conduite et les questions qu'elle soulève », Rapport du secrétariat, New-York, ONU, 1976, p.12. Voir également, M. Virally, « Les codes de bonne conduite, pour quoi faire ? » *in, Transfert de technologie, sociétés transnationales et nouvel ordre international*, Ed. J. Touscoz, PUF 1978.
[325] Initialement, toutefois, les codes de conduite internationaux se voulaient des codes obligatoires. C'est au fil des négociations entre les pays industrialisés et les pays en développement qu'ils sont devenus des instruments volontaires, en ce sens Veilleux A. et Bachand R., *Droit et devoirs des investisseurs : existe-t-il un espace juridique transnational ?,* Groupe de recherche sur l'intégration continentale, http://www.unites.uquam.ca/gric, p.8.
[326] Voir E. Claudel et B. Thullier, « Regard sur le droit mou », Revue de jurisprudence commerciale 2006 n° 1 p. 4 qui évoquent un mécanisme d'autorégulation. Voir également, plus généralement, C. Thibierge, « Le droit souple, Réflexion sur les textures du droit », RTDCiv. 2003, p. 599.

meilleure image d'elles-mêmes. « Les codes de conduite tendent à améliorer l'image des entreprises signataires auprès du public et fournissent aux entreprises des principes de gestion destinés à obtenir des gains de productivité »[327]. Et c'est en cela très certainement, que réside le deuxième avantage des codes de conduite. L'adhésion à un code de conduite constitue un atout en termes de concurrence. De ce point de vue, « le code de conduite apparaît essentiellement comme un instrument de promotion économique »[328]. C'est vrai des codes de conduite, c'est vrai également d'autres instruments volontaires, tels que les labels par exemple[329].

A ce titre, les codes de conduite revêtent indéniablement une certaine effectivité. Il est vrai que les codes de conduite sont surtout conçus comme des instruments d'autodiscipline dont l'efficacité est, par conséquent, étroitement liée au bon vouloir de leur destinataire. Il s'agit donc d'une efficacité relative dont il ne faut cependant pas négliger les effets. Dans la mesure où l'adhésion à un code de conduite est impulsée par la volonté d'asseoir une certaine crédibilité, la déviance d'un signataire peut ruiner l'effet recherché et conduire à la naissance d'un sentiment contraire encore plus fort que celui ressenti par un usager vis-à-vis d'une entreprise qui n'a pas pris d'engagements supplémentaires aux exigences légales mais qui respectent néanmoins ces dernières.

L'entreprise non respectueuse du code auquel elle a adhéré s'expose, en outre, à la désapprobation de ses concurrents et de ses partenaires. Il faut ainsi considérer, avec le Groupe de personnalités de l'ONU que « bien que de telles recommandations n'aient pas de caractère obligatoire, elles jouent le rôle d'un instrument de persuasion morale, renforcées qu'elles sont par l'autorité des organisations internationales et par la force de l'opinion publique »[330]. Il faut néanmoins reconnaître, qu'abordés sous cet angle, les codes de conduite demeurent des recommandations dépourvues de valeur juridique[331]. Il faut donc se demander si de tels codes peuvent être érigés au rang de source du droit, ce qui permettrait de les doter d'une force obligatoire et de sanctionner leur violation.

Les codes de conduite sont, *a priori*, susceptibles d'entrer dans plusieurs moules juridiques. On songe bien sûr à la convention, mais également à la coutume. Plus modestement, on peut se demander s'ils ne peuvent pas servir de référence à la définition de certains standards juridiques.

---

[327] J.-B. Racine, « La valeur juridique des codes de conduite privés dans le domaine de l'environnement », RJE 4/1996, p. 413.
[328] G. Farjat, *op. cit*., p. 52. Voir également, F. Bellivier et C. Noiville, « Code de conduite et équité des échanges de ressources biologiques », Idées pour le débat, n°10, 2006, p.7, http://www.iddri.org pour qui le code de conduite peut constituer pour les entreprises privées un outil de crédibilité.
[329] L. Boy, « L'éco-label communautaire, un exemple de droit postmoderne », Rev. int. dr. éco., 1996, p. 69.
[330] Doc. ONU E/5500, p. 62, cité par G. Farjat, *op. cit*., p.48
[331] V. M. Bettati, « Réflexion sur la portée du Code international de conduite pour le transfert de technologies : éloge de l'ambiguïté », *in Droit et Liberté à la fin du XX^e siècle*, Etudes offertes à C.-A. Colliard, Pédone, 1984, p. 83 et suiv.

Une convention. – Le processus d'élaboration d'un code de conduite privé fait immanquablement penser à celui qui préside à l'élaboration de la convention. Il y a bien discussion entre des partenaires qui conviennent de poser des règles destinées à gouverner leurs actions.

Il paraît néanmoins difficile de qualifier les codes de conduite de convention. La convention est un accord de volontés destiné à produire un effet de droit quelconque. Or, il paraît douteux de considérer que les auteurs de codes de conduite souhaitent leur faire produire des effets juridiques. Dans la plupart des cas, il est même précisé que les codes n'ont pas de valeur juridique contraignante pour ceux qui y adhèrent.

On peut imaginer que des partenaires reprennent, dans leur contrat, un code de conduite. Cette intégration procurerait ainsi au code de conduite la force obligatoire dont il est *a priori* dépourvu. On a parlé à ce titre de «contractualisation» des codes de conduite[332]. L'intérêt d'une telle démarche est de permettre d'engager la responsabilité contractuelle de la partie au contrat qui ne respecte pas ses engagements. Toutefois, cela suppose une démarche supplémentaire des parties et démontre, *a contrario*, que le code de conduite n'a pas cet effet à lui seul.

Naturellement, pour qu'un tel instrument soit opposable au cocontractant, il convient au préalable de s'assurer qu'il a eu connaissance de son existence et de son contenu. Or, il apparaît que même si une clause du contrat fait référence à un code de conduite, l'incluant donc *a priori* dans le champ contractuel, rien ne garantit qu'il soit pris en compte par le juge.

Ainsi, la clause contenue dans les conditions générales de fourniture d'accès à Internet, qui impose à l'abonné de respecter le code de bonne conduite des usagers, diffusé sur le site du fournisseur, sous peine de suspension ou de résiliation de l'accès au service, crée un déséquilibre significatif au détriment du consommateur, puisque ce dernier encourt des sanctions en cas de non-respect d'un code de bonne conduite dont il n'est pas établi qu'il en ait eu connaissance[333].

Il est évident que, ici comme en d'autres domaines, la qualité des parties n'est pas indifférente à la solution du litige ce qui réduit les potentialités de cette qualification. Une deuxième qualification juridique peut alors être envisagée, celle de coutume.

---

[332] F. Osman, « Avis, directives, codes de bonne conduite, recommandations, déontologie, éthique, etc. : Réflexion sur la dégradation des sources privées du droit », RTDCiv. 1995, p. 528.

[333] TGI Nanterre, Ch. 6, 3 Mars 2006, Association U/SA N. - T. JurisData n°2006-308052 ; Voir également, TGI Nanterre, Ch. 1, 9 Févr. 2006, union fédérale des consommateurs que choisir/SA FRANCE TÉLÉCOM, JurisData n° 2006-304649. De façon encore plus explicite, il a été jugé qu'est abusive, la clause qui permet d'exclure un usager du service Internet en cas de non-respect du code de bonne conduite disponible sur le site du fournisseur, puisque ce code n'est pas annexé au contrat et n'a donc pas été accepté expressément par l'usager : TGI PARIS, Ch 1 section sociale, 21 Févr. 2006, Association familles de France/SAS FREE, JurisData n° **:** 2006-295356.

Une coutume. – La qualification des codes de conduite en coutume permettrait de l'ériger au rang des sources directes du droit. Pour y parvenir, Gérard Farjat, dans sa « Réflexion sur les codes de conduite privés »[334], a proposé de recourir à la notion « d'autorité de fait »[335], empruntée au Doyen Carbonnier[336]. Ainsi, à l'instar du Doyen Carbonnier qui attribuait cette qualification à la jurisprudence et à la doctrine, on pourrait considérer que les codes de conduite fournissent « des éléments d'appréciation pour interpréter les règles de droit ou pour construire, dans le silence ou l'insuffisance de ces règles, la solution d'une difficulté ».

Rares sont aujourd'hui les auteurs à admettre qu'une telle qualification puisse s'appliquer à la jurisprudence, parce qu'elle est plus que cela[337]. En revanche, la qualification paraît tout à fait indiquée en ce qui concerne les usages[338]. Sous la qualification d'autorité de fait, on trouverait donc la doctrine, les usages et les codes de conduite.

La qualification d'autorité de fait permet de mettre en exergue les caractéristiques communes de ses composantes. La jurisprudence, par son travail d'interprétation du droit, peut transformer un usage ou une opinion doctrinale en une règle de droit en la faisant apparaître comme une coutume[339]. Est-il alors possible qu'une autre autorité de fait, le code de conduite, puisse de la même manière, être transformée en coutume ?

Beaucoup d'auteurs expriment des réticences face à une telle proposition. Pour le comprendre, il convient de rappeler que la coutume, pour exister, suppose la réunion de deux éléments : un élément matériel et un élément psychologique.

L'élément matériel consiste en la répétition d'un comportement : la formation d'une coutume suppose qu'une règle de conduite soit suivie de manière habituelle c'est-à-dire appliquée plusieurs fois. La durée constitue donc un élément essentiel dans la formation d'une coutume. L'élément psychologique, c'est l'adhésion du groupe auquel s'applique la coutume. La coutume doit donc être ressentie comme un comportement obligatoire par l'opinion commune. Par conséquent, une règle de conduite ne devient une coutume que lorsque le groupe social considère sa violation comme manifestant le non-respect d'une règle de droit. Le plus souvent, cela se manifestera lorsque l'autorité judiciaire est amenée à sanctionner la violation de la coutume.

---

[334] G. Farjat, *op. cit*., p. 61.
[335] Par opposition à la notion d'autorité de droit.
[336] J. Carbonnier, *Droit civil, introduction*, PUF 1ère éd. 1955, rééd. en 2004, n°144, p.273.
[337] La doctrine dominante considère que la jurisprudence est une source indirecte du droit V. P. Malaurie et P. Morvan, Droit civil, Introduction générale, n° 346 s., Defrénois, 2ème éd. 2005.
[338] Les usages conventionnels sont « des usages suivis dans certains contrats dérivant d'anciennes clauses de style aujourd'hui sous-entendues, qui tirent leur force obligatoire de la volonté tacite des contractants et n'ont qu'une valeur supplétive », Cornu G. (Dir.), « Vocabulaire juridique », Travaux association Henri Capitant, PUF, 8ème éd. 2007.
[339] M. Pédamon, « Y a-t-il lieu de distinguer les usages et les coutumes en droit commercial ? », RTD com. 1959, p. 335

Les deux éléments doivent être réunis. En effet, certains comportements se répètent mais ils ne sont pas pour autant considérés comme obligatoires. Ainsi en est-il des étrennes ou du pourboire. Il s'agit ici d'un usage et non d'une coutume.

On comprend alors les réticences à adhérer à l'idée qu'un code de conduite puisse être qualifié de coutume. La proposition oblige, *a priori,* à admettre la théorie de la formation instantanée de la coutume proposée par Boris Starck[340], ce que peu d'auteurs sont prêts à faire.

Il convient donc d'explorer une troisième voie. Les codes de conduite peuvent également servir de référence pour la définition de standards juridiques.

Une référence pour la définition de standards juridiques. – Si la qualification de coutume laisse d'aucuns perplexes, la référence à celle de standard juridique suscitera sans doute davantage d'engouement[341]. Les directives contenues dans les codes de conduite paraissent, en effet, pouvoir nourrir les standards juridiques tels que la faute, la bonne foi ou encore les bonnes mœurs par exemple. « Les juges peuvent utiliser des dispositions émanant de codes de conduite comme éléments d'interprétation ou de construction de solutions juridiques sans même faire référence à leur source d'inspiration ».[342]

Ainsi, pour apprécier la faute, les juges vont s'attacher au comportement du bon père de famille, ou en l'occurrence, au comportement du bon professionnel. Or, on sait que ce comportement, n'est pas toujours aisé à définir. Précisément, les codes de conduite peuvent aider les juges dans cette quête dans la mesure où ils comportent et définissent des engagements de prudence et de diligence qui, qualifiés d'usage, permettent de créer de « véritables obligations juridiques de prudence et de diligence »[343].

Des travaux antérieurs[344] ont expliqué que, sur cette base, il devrait être possible de sanctionner l'auteur d'un dommage écologique ou l'auteur de faits de concurrence déloyale. Dans les deux cas, on peut imaginer que le juge s'appuie sur les règles contenues dans un code de conduite pour apprécier et caractériser une faute à l'origine du dommage. Dans le même ordre d'idée, les codes de conduite peuvent s'avérer utiles dans la définition et l'appréciation de la notion de bonne foi. Ainsi, on peut légitimement se demander si le signataire d'un code de bonne conduite qui ne respecte pas ses engagements ne fournit pas une apparence trompeuse de la réalité.

---

[340] B. Starck, « A propos des accords de Grenelle, Réflexions sur une source informelle du droit » : JCP 1970, I, 2363.
[341] Voir K. J. Hopt, « Le gouvernement d'entreprise – Expériences allemandes et européennes », Revue des sociétés 2001, n° 1, p. 3 qui évoque cette notion de standard comme un modèle, sans force obligatoire, mais complémentaires à des textes de loi.
[342] G. Farjat, *op. cit*., p. 63.
[343] J.- B. Racine, *op. cit*. p. 419.
[344] J.- B. Racine, *op. cit*. p. 419 et suiv.

Quoi qu'il en soit, l'outil séduit dans le domaine de la protection des données personnelles. Ainsi, l'opérateur télécom Orange, dont les réseaux, tant mobiles que fixes, acheminent une quantité croissante de données personnelles, a signé une charte pour la protection des données personnelles. L'ambition d'Orange est d'être reconnue par ses clients, ses utilisateurs et ses partenaires comme « opérateur de confiance ». Pour cela, le Groupe a pris des engagements clairs et fermes en matière de protection des données personnelles et de respect de la vie privée de ses clients.

Le 7 novembre 1013, à l'occasion du Show Hello 2013, Stéphane Richard a officiellement signé une charte comportant 4 engagements vis-à-vis des clients sur la protection de leurs données personnelles et de leur vie privée :

- **« la sécurité** des données personnelles des clients à travers la fiabilité de leur traitement et la sécurité de leur conservation
- **le contrôle** par les clients de leurs données personnelles et de l'utilisation qui en est faite, notamment, *via* un **tableau de bord personnel**
- **la transparence** du traitement des données de ses clients et utilisateurs dans toutes les étapes de la relation
- **l'accompagnement de tous ses clients et utilisateurs** pour les aider à protéger leur vie privée et à mieux gérer leurs données personnelles »

Il existe également des initiatives fondées sur l'éthique des professionnels du recrutement :

- Charte réseaux sociaux, Internet, vie privée et recrutement du 14 novembre 2010 (MEDEF, ANDRH, Syntec recrutement, Viadeo). Les signataires de la charte s'engagent à privilégier l'utilisation des réseaux sociaux professionnels et non personnels, à ne pas utiliser les moteurs de recherche, les réseaux sociaux afin d'enquêter sur leur futur salarié, et à alerter les utilisateurs de ces sites à vérifier au préalable s'ils ont la possibilité de supprimer les données qu'ils ont mis en ligne et de faire valoir leur droit à l'oubli numérique.

- Charte du droit à l'oubli dans les sites collaboratifs et les moteurs de recherche du 13 octobre 2010 (Benchmark Groupe – Copainsdavant, Pages Jaunes – 123 people, Skyrock, Microsoft France – MSN, Windows live, Bing). Les deux géants du secteur Google et Facebook ont refusé de signer cette charte du droit à l'oubli numérique.

Il convient également d'évoquer la charte de déontologie « Publicité ciblée et protection des internautes » du 30 septembre 2010, signée par dix associations professionnelles et

proposant des mécanismes innovants d'organisation collective des professionnels, destinés à recueillir et à respecter les souhaits exprimés par les internautes. Les recommandations contenue dans la charte concernent notamment l'information des internautes, l'exercice de leurs droits en matière de publicité ciblée, le rapprochement entre les données de navigation et les données personnelles, la publicité géo-localisée, le *capping* (maîtrise de l'exposition à la publicité) et la protection des publics mineurs. La charte recommande également de limiter la durée d'exploitation des cookies de publicité comportementale à une durée, par défaut, de 60 jours, sans toutefois exclure l'application de durées plus courtes ou plus longues, proportionnées à la durée du cycle d'achat des produits ou services.

Les réseaux sociaux et les moteurs de recherche se dotent également de politiques de confidentialité et d'utilisation des données personnelles afin de prévenir l'internaute des conséquences de ses actions ayant pour finalité la fourniture d'informations. Néanmoins, ces politiques sont largement controversées et critiquées. Le 5 septembre 2013, aux Etats-Unis, six organisations de protection des libertés et de la vie privée ont saisi la *Federal Trade Commission* (FTC), l'autorité américaine de la concurrence. Pour elles, la politique de Facebook qui venait d'être à nouveau modifiée, permet plus facilement au réseau social d'utiliser les données personnelles de ses utilisateurs, y compris des mineurs, pour faire de la publicité sur le site.

Plus récemment, le 25 mars 2014 précisément, *l'UFC-Que choisir ?,* une association de consommateurs d'Europe Occidentale créée en 1951, assigne devant le TGI de Paris Facebook, Twitter et Google+ pour clauses jugées « abusives », celles-ci permettant une utilisation « tentaculaire » et « à l'infini » des données personnelles. L'association demande « au juge français d'ordonner la suppression ou la modification des clauses litigieuses imposées par ces sociétés »[345].

Il est bien évident que même si les codes de conduite ne comportent pas, en leur sein, de règles juridiques contraignantes, en théorie, leur violation expose leur auteur à des sanctions. Pour autant, il n'en sera ainsi, en pratique, que si les juges acceptent de s'appuyer sur les codes de conduite privés dans leur mission d'application et d'interprétation de la règle de droit ce qui conduit naturellement à se pencher sur les difficultés liées à la sanction effective des codes de conduite privés.

[345]http://www.lemonde.fr/technologies/article/2014/03/25/donnees-personnelles-l-ufc-assigne-twitter-facebook-et-google-pour-clauses-abusives_4389172_651865.html

2.3. Les sanctions

L'effectivité du droit à l'oubli, quelle que soit la forme qu'on lui donnera (droit subjectif ou droit dérivé de l'effacement, durée limitée de conservation des données, retrait….) se mesurera à l'aune des sanctions de sa violation. Cet aspect est au cœur du dispositif de protection des données personnelles. Une sanction dissuasive encouragera au respect des droits des titulaires des données. La Commission européenne dans sa communication du 4 novembre 2010 a rappelé cette nécessité[346]. A cette finalité comminatoire, s'ajoute l'indemnisation des préjudices causés. Il convient donc d'envisager l'effectivité des sanctions qui pourraient résulter de l'inclusion d'un droit à l'oubli dans un code de conduite d'une part et, d'autre part, celle des sanctions rattachables à un dispositif plus contraignant, tel que le dispositif de protection des données à caractère personnel.

2.3.1. Les difficultés liées à la sanction effective des codes de conduite

Admettre qu'un code constitue une autorité de fait proche des usages ne suffit pas à en garantir l'effectivité. Les codes de conduite public ne semblent d'ailleurs pas mieux lotis parce qu'il n'existe pas de véritable différence de nature entre les codes publics et les codes privés. Un code de conduite adopté par une autorité publique « n'a, en droit, pas davantage de force qu'un code émanant d'une organisation purement privée ».[347]

Dans les faits pourtant, il est vrai que leur situation est un peu différente dans la mesure où l'autorité publique dispose d'instruments dont la mise en œuvre peut assurer l'efficacité du code et, sans doute le juge est-il plus enclin à se référer au contenu d'un code émanant de l'autorité publique. Il s'agit cependant de circonstances périphériques au code, circonstances qui n'en modifient pas la nature.

Comment donc le juge appréhende-t-il le code de conduite privé ? C'est à cette question qu'il faut tenter de répondre en envisageant la manière dont il peut appliquer des sanctions civiles mais également des sanctions pénales.

2.3.1.1. Les sanctions civiles

Si certaines dispositions contenues dans les codes de conduite peuvent être qualifiées d'usage, le juge civil sera amené à en tenir compte. Il est vrai que cette position est relativement récente. Longtemps, le juge civil a refusé d'intégrer dans son appréciation, les règles

[346] Une approche globale de la protection des données à caractère personnel dans l'Union européenne, spéc. p. 10 et s.
[347] G. Farjat, *op. cit*., p. 50.

déontologiques contenues dans les codes, en ce compris les codes officialisés par la voie d'un décret[348]. Il a ainsi été jugé que la violation d'une règle du code de déontologie médicale ne peut entraîner que des sanctions disciplinaires et ne saurait justifier l'annulation du contrat constitutif de cette violation.

Cette position peut paraître cohérente en ce qu'elle fait fi de l'*instrumentum* pour ne s'attacher qu'au *negotium*. L'aval de l'autorité publique ne changerait donc rien à la nature juridique première du code. Pour autant, pareille conception semble contestable dans la mesure où les codes de bonne conduite revêtant la forme d'un décret constituent des règlements administratifs et les sanctions qu'ils prévoient apparaissent comme des actes administratifs individuels susceptibles de recours en annulation devant la juridiction administrative. « Cette édiction revêt le caractère d'une réception d'une norme émanant d'un ordre juridique privé par l'ordre juridique étatique (…) », réception qui intègre les règles contenues dans le code « dans la pyramide des normes sécrétées par la puissance publique étatique »[349]. Cette intégration devrait donc permettre au juge de sanctionner l'acte juridique contraire aux règles de bonne conduite contenues dans un code officialisé par décret.

C'est précisément la position du Conseil d'Etat qui, depuis de nombreuses années déjà, reconnaît une valeur juridique aux codes privés faisant l'objet d'un agrément ministériel[350]. Pour qu'il en soit ainsi, l'ordre professionnel privé doit être investi d'une mission de service public, doté de prérogatives de puissance publique, et l'acte litigieux doit procéder de l'usage de ces prérogatives[351]. La Cour de cassation semble toutefois avoir adhéré à cette distinction et être revenue à une position moins stricte. C'est ainsi qu'elle admet que le code de déontologie médicale puisse être invoqué par le demandeur d'une action en dommages-intérêts dirigée contre un médecin[352].

Faut-il en conclure que les codes de conduite purement privés – à savoir les seuls que l'on rencontre sur la question du droit à l'oubli – doivent être systématiquement écartés par les juridictions de l'ordre civil ? Rien n'est moins sûr.

En France, le code civil lui-même, à l'article 1135, privilégie le contenu de l'acte en invitant le juge chargé de l'examen d'un contrat à tenir compte de « toutes les suites que l'équité, l'usage ou la loi donnent à l'obligation d'après sa nature ». Précisément, les codes de conduite paraissent pouvoir endosser la qualification d'usage conventionnel puisqu'ils portent des recommandations dégagées sur la base d'un consensus. Cette qualification n'a

[348] V. Cass. Soc., 24 mai 1960, JCP G 1961, II, 12044, note J. Savatier.
[349] F. Osman, *op. cit*., p. 518.
[350] Arrêt Bouguen, CE, 2 avril 1943, JCP G 1944, II, 2565, note C. Célier ; S. 1944, 3, 1 concl. Lagrange et note Mestre.
[351] F. Osman, *op. cit*., p. 519.
[352] Cass. 1ère civ., 18 mars 1997, JCP 1997, II, 22829, P. Sargos.

naturellement pas pour effet d'ériger les codes de conduite au rang de norme juridique obligatoire mais elle leur permet d'être intégrés dans le champ contractuel au même titre que la prudence ou la diligence dont on tire de véritables obligations. Ce n'est donc que si les parties manifestaient la volonté d'écarter cet usage, que l'on devrait l'exclure du champ contractuel.

C'est en ce sens que s'est prononcée la cour d'appel de Poitiers au sujet de la pratique du spamming. Le spamming consiste à envoyer des messages sur Internet non sollicités par les destinataires. Il s'agit d'une pratique déloyale qui peut être à la source de graves perturbations. En effet, la Netiquette, qui est le code de bonne conduite sur Internet, reconnue et admise dans la communauté des internautes, prohibe cette pratique qui perturbe gravement l'équilibre du réseau et provoque l'encombrement des messageries avec un coût pour l'internaute qui doit procéder à la suppression de ces messages non désirés. C'est en considération de ces éléments que la Cour a considéré comme justifiée, la résiliation du contrat d'abonnement par l'opérateur pour inexécution fautive du contrat par l'abonné qui a pratiqué le spamming dans le cadre de l'utilisation du contrat, sur différents forums de discussion, en vue de développer ses activités commerciales, et a persisté dans son comportement, malgré les mises en garde de l'opérateur[353].

Si, en matière civile, la jurisprudence ouvre quelques perspectives, la situation est un peu plus complexe en matière pénale.

2.3.1.2. Les sanctions pénales

En principe, même si un code de conduite peut être qualifié d'usage, la violation d'une disposition contenue dans un code de bonne conduite ne devrait pas pouvoir donner lieu à une sanction pénale. En effet, le principe de légalité criminelle, dont il résulte qu'une sanction pénale ne peut être prononcée que si elle est prévue par un texte de loi, paraît s'y opposer.

Pour autant, malgré ce principe, les juridictions pénales ont parfois été conduites à sanctionner pénalement un comportement contraire à un usage[354]. Ainsi, en 1967, une condamnation pénale pour fraude et falsification fût approuvée par la chambre criminelle de la Cour de cassation alors que celle-ci reposait sur le constat de la violation d'un usage[355]. Plusieurs autres décisions approuvant la qualification de tromperie[356] ou encore de faux en écriture privée ou de fraude fiscale[357] ont par la suite été rendues.

---

[353] Cour d'appel POITIERS, Chambre civile 1, 11 Mai 2004, Gueret/Société Wanadoo interactive, JurisData n° 2004-252027, arrêt que l'on peut rapprocher des jugements de 2006 cités note 15.
[354] Voir V. Wester-Ouisse, « Le droit pénal face aux codes de bonne conduite », Rev. Sc. Crim. 2000, p. 351 et suiv. spéc. p. 357.
[355] Cass. Crim., 5 oct. 1967, Bull. crim. n°242.
[356] Cass. Crim. 15 janv. 1985, Bull. crim. n° 26 ; 7 fév. 1994, Bull. Crim. n°54.
[357] Voir V. Wester-Ouisse, *op. cit*,. et *loc.cit.*

A l'évidence, il n'est pas question de recourir de façon systématique aux règles contenues dans les codes de conduite mais uniquement dans les hypothèses où la réglementation légale fait défaut. Comme en matière civile, les codes de conduite peuvent guider le juge répressif confronté à une disposition légale au contenu trop flou ou trop général.

Le constat n'a pas pour effet de limiter l'atteinte au principe de la légalité des infractions et des peines. « Affirmer que compte tenu des textes existants, une personne n'est pas coupable de fraude, n'est pas un déni de justice »[358]. S'en remettre aux usages pour apprécier un comportement et le sanctionner pénalement peut alors paraître excessif.

D'aucuns objecteront qu'une telle vision des codes de conduite s'oppose à toute idée de systématisation et rend discutable l'efficacité juridique des codes : tout code de conduite ne peut être considéré comme une coutume et rien ne garantit que les règles contenues dans un code de conduite serviront réellement à étoffer les standards juridiques. C'est là sans doute la limite de la proposition et, d'une façon plus générale, celle de l'efficacité des codes de conduite.

2.3.2. Les sanctions résultant du dispositif de protection des données à caractère personnel

En France, il revient à la CNIL la mission de veiller au respect des données personnelles, aux tribunaux et à la responsabilité civile, celle d'indemniser. Le droit positif ne dote pas le droit à l'oubli d'un régime singulier. Il est soumis aux mêmes règles que celles qui protègent l'ensemble des droits instaurés par la loi informatique et libertés. Les institutions européennes partagent la même analyse. Certes le droit à l'oubli pourrait être qualifié de droit substantiel. Il ne mérite cependant pas une place distincte des autres droits des utilisateurs. Une égalité de traitement au niveau des sanctions serait donc préférable.

2.3.2.1. Les sanctions administratives

La loi de 1978, tout comme le Parlement et la Commission européenne, paraissent privilégier les sanctions administratives. La réforme que préconisent les institutions européennes reste sur la même ligne que le droit positif français. Cette politique témoigne de la place qu'occupe la protection des données personnelles dans l'ordonnancement juridique. Elle ne s'arrête pas aux intérêts privés. Elle est également une question d'intérêt général. Les pouvoirs publics français font pour le moment le pari de la régulation. Ce contrôle administratif est important car les juridictions françaises demeurent relativement peu saisies de ces questions.

[358] V. Wester-Ouisse, *op. cit*,, p. 358.

La volonté de la Commission européenne de le durcir et d'accroître les pouvoirs de l'autorité de contrôle doit être approuvée.

Le présent - La CNIL est l'organisme de contrôle de l'usage des données personnelles en France. Elle est dotée de pouvoirs significatifs, renforcés par la loi du 6 août 2004, en application de l'article 28-3 alinéa 2 de la directive de 1995 qui disposait justement que l'autorité nationale de contrôle doit disposer « de pouvoirs effectifs d'intervention » à l'instar de celui « d'ordonner le verrouillage, l'effacement ou la destruction de données ou interdire temporairement ou définitivement un traitement, ou celui d'adresser un avertissement ou une admonestation au responsable du traitement ». Le législateur français a pris acte de cette recommandation, en élargissant les pouvoirs d'investigation de la CNIL et en diversifiant les sanctions encourues.

Investigations - La première difficulté à laquelle la CNIL peut être confrontée consiste à identifier les manquements. A cette fin, elle dispose d'un large pouvoir d'investigation[359], encore accru par la loi dite Hamon, n°2014-344 du 17 mars 2014. Le législateur établit un juste équilibre entre les pouvoirs d'investigation de la CNIL et les garanties accordées aux personnes objet du contrôle. Elle peut « s'autosaisir »[360] et effectuer d'elle-même des contrôles sur place et sur pièces. Le ministère public est informé préalablement de toute mesure de contrôle[361]. Si la personne, sujet du contrôle, n'a pas à être préalablement prévenue de celui-ci, elle peut toutefois s'y opposer dès qu'elle en a connaissance. Afin de passer outre ce refus, la CNIL peut solliciter l'autorisation du juge des libertés et de la détention du tribunal de grande instance dans le ressort duquel sont situés les locaux à visiter. D'aucuns plaident pour une autorisation judiciaire systématique préalablement à toute visite[362]. L'utilité de cette condition supplémentaire, qui risque de générer lenteur et encombrement des tribunaux, est discutable. La pertinence du contrôle de l'autorité administrative suppose que cette dernière ne soit pas enserrée dans un carcan de règles trop contraignantes. La pratique actuelle laissant à la CNIL le soin d'apprécier l'opportunité d'une autorisation judiciaire devrait être prolongée, tant qu'un droit à recours *a posteriori* contre ses décisions est maintenu.

---

[359] E. Papin, « L'application de la loi informatique et libertés du 6 janvier 1978 par les AAI dans le cadre de leurs opérations de saisie », Rev. Lamy dr. immat. mars 2010, n° 58, p. 49.

[360] CE, ord. réf., 19 févr. 2008, n° 311974, Jurisdata n° 2008-073370 : cette possibilité pour la commission de s'autosaisir n'est pas contraire à l'exigence d'équité consacrée par la Convention européenne des droits de l'homme.

[361] Article 44. Sur le détail de ces mesures, voir R. Perray, « Traitements de données à caractère personnel », Jurisclasseur adm., fasc 274, 2012.

[362] En faveur d'une autorisation judiciaire préalable : La proposition de règlement européen relatif aux données à caractère personnel : proposition du réseau Trans Europe experts, sous la direction de N. Martial-Braz, *op. cit.*, n° 75.

Le Conseil d'Etat veille au respect de ce droit de refus du propriétaire des lieux visités. La seule mention sur le procès-verbal que l'information sur le droit d'opposition a été donnée a été jugée contraire à l'article 8 de la CEDH. Une preuve directe et positive du respect de cette obligation est exigée[363]. La violation de cette dernière a justifié l'annulation d'une décision de sanction financière de 50 000 euros prise par la CNIL. L'opposition à la visite demeurera cependant sans effet « lorsque l'urgence, la gravité des faits à l'origine du contrôle ou le risque de destruction ou de dissimulation de documents le justifie »[364].

Ce droit d'opposition appartient au seul propriétaire des lieux ou au gérant de l'entreprise, ou une personne dûment mandatée par ces derniers. Le fait pour un tiers d'obstruer illégitimement les investigations de la CNIL est constitutif du délit d'entrave[365]. En matière de recherche dans le domaine de la santé, la sanction est plus drastique, puisqu'elle peut consister dans le retrait temporaire ou définitif de l'autorisation délivrée par la CNIL[366]. Ce droit d'opposition demeure *a priori* peu exercé par les intéressés. Depuis 2011, on dénombre moins d'une dizaine d'oppositions et toutes ont été levées par le juge[367].

Constats en ligne - Jusqu'à il y a peu, la loi ne prévoyait pas la possibilité pour la CNIL d'opérer des constats en ligne. A cette fin, elle devait s'adjoindre les services d'un huissier[368]. La loi Hamon pallie cette lacune. Désormais, la CNIL pourra « à partir d'un service de communication au public en ligne, consulter les données librement accessibles ou rendues accessibles, y compris par imprudence, par négligence ou par le fait d'un tiers, le cas échéant en accédant et en se maintenant dans des systèmes de traitement automatisé de données le temps nécessaire aux constatations ». En outre, elle « peut retranscrire les données par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle»[369]. Certes, ce pouvoir, qui vise à rendre plus efficaces et rapides les contrôles de la CNIL, reste limité aux

[363] CE, 6 nov. 2009, n° 304300 et n° 304301, D. act. 10 nov. 2009, note J.-M. Pastor ; JCP G 2010, 98, note J.-G. Sorbara ; Rev. Lamy dr. immat. janv. 2010, n° 56, p. 22, note M. Gaudemet ; Comm. comm. électr. 2010, comm. 19, note E.-A. Caprioli. Sur la contestation du contenu du PV, voir plus généralement : CE, 27 juill. 2012, n° 340026, Jurisdata n° 2012-016856 ; JCP A 2012, act. 570, note C.-A. Dubreuil.

[364] Article 44-II et articles 57 et suivants du Décret du 20 octobre 2005.

[365] Selon l'article 51 de la loi informatique et libertés, le fait d'entraver l'action de la commission dans le cadre de ses pouvoirs de contrôle de la mise en œuvre des traitements est puni d'un an d'emprisonnement et de 15 000 EUR d'amende relevant de la loi "informatique et libertés".

[366] Article 60 de la loi informatique et libertés.

[367] Th. Dautieu, Jurisclasseur comm., « La commission nationale de l'informatique et des libertés, saisine par les particuliers, pouvoirs de contrôle et de sanction », spéc. n° 43 : concernant les demandes d'ordonnances "préventives", la pratique est encore plus exceptionnelle. Seules cinq demandes ont été formulées par la CNIL, systématiquement pour des contrôles s'inscrivant dans le cadre d'instruction de plaintes dont la teneur des échanges avec le responsable de traitement et la gravité des faits pouvaient laisser supposer un risque de destruction ou de dissimulation des documents.

[368] Pour une sanction infligée sur la base d'un tel constant, voir CNIL, délib. n° 2012-320, 20 sept. 2012, portant avertissement public à l'encontre de la commune de Montreuil.

[369] Article 44.

données accessibles ou rendues accessibles. Néanmoins, s'agissant de la question du droit à l'oubli, elle offre un atout majeur puisque pour l'essentiel, ce sont les données accessibles qui sont concernées.

Plaintes des utilisateurs - La CNIL peut également être informée de manquements par le biais de plaintes des particuliers auxquels on refuse l'accès, la rectification ou la suppression de leurs données personnelles[370]. Cette plainte n'est recevable qu'après l'expiration d'un délai de deux mois suite à une mise en demeure infructueuse. Les plaintes peuvent désormais se faire sur le site Internet de la CNIL. Cette dernière n'est pas tenue d'y donner suite[371]. Le principal motif de saisine de la commission semble être l'opposition à figurer dans un fichier, tous secteurs confondus[372]. Il s'agit évidemment d'un point important pour les utilisateurs, l'enquête sociologique ayant révélé une sorte de fatalisme des usagers qui semblent considérer que face aux services en ligne, ils ne disposent que de peu d'armes.

Coopération avec d'autres autorités de contrôles – Enfin, toujours dans l'objectif de renforcer le contrôle de la CNIL, le législateur a conforté son pouvoir de s'associer les services d'autres autorités de contrôles. Par exemple, depuis 2011, elle peut être saisie par le défenseur des droits d'une réclamation dont lui-même a été saisi[373]. La coopération avec la Direction générale de la concurrence, de la consommation et de la répression des fraudes, ci-après DGCCRF, a également été officialisée par la loi Hamon. L'article 76 de la loi n°2014-344 du 17 mars 2014 vient ainsi modifier la rédaction de l'article L.141-1 du Code de la consommation, qui dispose désormais que : « dans l'exercice de leurs missions, les agents mentionnées au II de l'article L. 450-1 du code de commerce sont habilités à constater les infractions et manquements aux chapitres II, IV et V de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et peuvent communiquer ces constatations à la Commission nationale de l'informatique et des libertés ». Ce partenariat est emblématique de la volonté du législateur de veiller au respect de la législation sur les données personnelles. La DGCCRF est en effet dotée de moyens supérieurs à ceux de la CNIL. Ainsi d'après le dernier rapport d'activité en 2012, là où la CNIL n'a pu opérer que quelques centaines de contrôles, la DGCCRF en a réalisé 137000.

---

[370] Article 11, 2° c.

[371] Un recours pour excès de pouvoir contre cette décision demeure envisageable. Voir par exemple : CE, 5 déc. 2011, n° 319545, Jurisdata n° 2011-027474, pour l'arrêté du 22 août 2001 portant création d'un traitement relatif à la délivrance des visas dans les postes diplomatiques et consulaires pour en permettre l'instruction et procéder à l'échange d'informations avec des autorités étrangères.

[372] Th. Dautieu, art. préc., n° 9 : cela représente 46 % des plaintes reçues en 2012.

[373] Article 9 de la loi organique n° 2011-333 du 29 mars 2011, relative au défenseur des droits. Le Défenseur des droits peut accompagner cette transmission de ses observations et demander à être informé des suites données à celles-ci.

Enfin, une coopération au niveau international est également prévue. Ainsi la CNIL peut être saisie d'une demande de la part d'une autorité exerçant des compétences analogues aux siennes dans un autre état membre de l'Union européenne afin qu'elle exerce ses pouvoirs de vérification[374].

La CNIL peut enfin saisir directement le ministère public lorsqu'elle estime que les faits relèvent d'une qualification pénale[375].

La diversité des sanctions - Lorsqu'une infraction est constatée, la palette des mesures que peut prononcer la CNIL est variée et graduée : du simple avertissement à des sanctions financières, qu'elle peut rendre publics ou non. Cette évolution accusée par la loi de 2004 a eu pour conséquence d'assimiler la CNIL à un tribunal. En corollaire, elle doit veiller au respect du contradictoire et des droits de la défense[376].

Avertissement, mise en demeure – L'avertissement est la sanction la plus « faible »[377]. Il a pour objet d'informer le responsable du traitement de la violation constatée. Généralement, il est accompagné d'une mise en demeure de se conformer à la loi informatique et libertés dans un délai fixé par la CNIL. Cette dernière peut directement mettre en demeure le responsable[378]. Le non-respect de celle-ci, dans le délai fixé, qui peut être réduit à cinq jours en cas d'urgence, autorise la CNIL à prononcer des sanctions plus lourdes[379]. Le responsable du traitement encourt alors, au choix de l'autorité administrative, une injonction de cesser le traitement[380], lorsque celui-ci est soumis à déclaration à la CNIL, un retrait de l'autorisation accordée en application de l'article 25[381] ou une sanction financière[382]. La reprise du traitement est généralement conditionnée à la mise en conformité avec le droit positif.

---

[374] Article 49 de la loi informatique et libertés. Pour une application : R. Dana, Manque de coopération et de transparence : la CNIL condamne Tyco Health care France à une amende de 30.000 euros, Comm. Comm. électr. N° 7, alerte 111.

[375] Cass. crim., 14 mars 2006, n° 05-83.423, Jurisdata n° 2006-032892.

[376] Voir dernièrement : CE, 12 mars 2014, n° 353193, AJDA 2014, p. 590.

[377] Pour un avertissement et une publicité : Délib. CNIL 2013-173 du 19 juin 2013, PARIBAS

[378] CE, 27 juill. 2012, n° 340026 *:* la CNIL est autorisée à « infliger un avertissement et à adresser simultanément une mise en demeure sur des faits postérieurs à l'avertissement et distincts de ceux-ci »

[379] La procédure de mise en demeure semble cependant être efficace puisque 90 % des mises en demeure auraient été suivies d'une mise en conformité du responsable de traitement, la CNIL clôturant alors le dossier : T. Dautieu, art. préc., n° 64.

[380] T. Dautieu, art. préc., n° 90 : le pouvoir d'injonction est rarement utilisé, les responsables de traitement se conformant très majoritairement aux mises en demeure qui leur sont adressées. Pour une illustration, voir toutefois : CNIL, délib. n° 2011-238, prononçant une sanction pécuniaire publique et une injonction de cessation de traitement à l'encontre de l'association LEXEEK éditeur du site www.lexeek.com.

[381] Ce pouvoir semble avoir été mis en œuvre pour la première fois en 2010. Voir : CNIL, délib. n° 2010-072, 18 mars 2010. - CNIL, communiqué, La CNIL ordonne l'interruption d'un dispositif biométrique illégal, 20 mai 2010 : interruption pour une durée de trois mois d'un dispositif biométrique qui avait été mis en place malgré le rejet de la demande d'autorisation qui avait été déposé par l'organisme déclarant. Voir également : Délib. CNIL 22 avril 2010 de la formation restreinte décidant de l'interruption de la mise en œuvre d'un traitement par la société X...

[382] Pour une application du cumul des diverses sanctions : affaire LEXEEK à propos du non-respect du droit d'opposition. Ce cumul reste cependant assez marginal. La CNIL fait un usage modéré de son pouvoir d'injonction : Th. Dautieu, art. préc., n° 90.

Sanctions financières – Le montant de la sanction pécuniaire que peut infliger la CNIL, telle que prévue au I de l'article 45, est proportionné à la gravité des manquements commis et aux avantages tirés de ce manquement. Ces critères larges englobent notamment les gains réalisés et les économies faites grâce à la violation constatée. Ce mode de calcul se veut plus dissuasif qu'une évaluation sur la base d'un préjudice avéré[383]. Néanmoins, les sanctions demeurent plafonnées. Lors du premier manquement, la condamnation ne peut excéder 150 000 euros[384]. En cas de manquement réitéré dans les cinq années à compter de la date à laquelle la sanction pécuniaire précédemment prononcée est devenue définitive, il ne peut excéder 300 000 euros ou, s'agissant d'une entreprise, 5 % du chiffre d'affaires hors taxes du dernier exercice clos dans la limite de 300 000 euros[385]. Ces sommes pourront paraître faibles à certaines entreprises. La CNIL se montre relativement modérée. Elle ne fait usage de cette sanction qu'avec parcimonie. La condamnation la plus élevée qu'elle ait prononcée ne dépasserait pas 150.000 euros[386].

Articulation avec les sanctions judiciaires – En outre, ces sommes n'ont pas vocation à se cumuler avec les condamnations pénales éventuelles. Ainsi, lorsque la commission a prononcé une sanction pécuniaire avant que le juge pénal ait statué sur les mêmes faits ou des faits connexes, celui-ci peut ordonner que les sommes prévues par la CNIL s'imputent sur l'amende qu'il prononce[387].

La loi informatique et libertés a prévu un arsenal de sanctions pénales. Ainsi, pour les traitements soumis à formalités préalables, le fait de ne pas procéder aux formalités requises est passible d'une peine de cinq ans d'emprisonnement et de 300 000 euros d'amende[388], cette dernière sanction pouvant aller jusqu'à 1 500 000 euros lorsque le responsable de traitement est une personne morale[389]. L'article 226-19-1 du Code pénal prévoit également qu'en matière de données personnelles collectées dans le cadre de recherches médicales, est puni de cinq ans d'emprisonnement et 300 000 euros d'amende le fait de procéder à un traitement dans deux cas. Soit il n'a pas préalablement informé individuellement les personnes sur le compte desquelles des données personnelles sont recueillies ou transmises de leur droit d'accès, de rectification et

[383] Th. Dautieu, art. préc., n° 86 : les sanctions pécuniaires représentent moins de la moitié des sanctions prononcées par la formation restreinte de la commission puisqu'elles ne peuvent intervenir qu'en cas de non-respect, par un responsable de traitement, d'une mise en demeure qui lui a été préalablement adressée.
[384] Pour une condamnation à un euro symbolique, voir délib. CNIL 2012-475 du 3 janvier 2013, Syndicat des copropriétaires « Arcade Champs Elysées ».
[385] La CNIL n'a fait usage de ses pouvoirs de sanction, en cas de récidive, qu'en juin 2010, à l'encontre d'une société ayant pour activité l'envoi à des particuliers de fax publicitaires non-sollicités, voir : CNIL, délib. n° 2010-232, 17 juin 2010
[386] Voir déjà : A. Debet, « Affaire Google Street View, une sanction exemplaire… mais quelles suites ? », Comm. com. électr. janv. 2012, étude 1. Pour d'autres exemples, voir, R. Perray, art. préc., p. 142
[387] Article 47 alinéa 3 de la loi informatique et libertés. Sur cette question, voir : F. Mattatia, « CNIL et Tribunaux : concurrence ou complémentarité dans la répression des infractions à la loi informatique et libertés », RSC 2009, p. 317.
[388] Article 226-16 et 226-16-1-A du Code pénal.
[389] Article 131-38 et 226-24 du Code pénal.

d'opposition, de la nature des informations transmises et des destinataires des données. Soit il a procédé au traitement malgré l'opposition de la personne concernée ou, lorsqu'il est prévu par la loi, en l'absence du consentement éclairé et exprès de la personne, ou, s'il s'agit d'une personne décédée, malgré le refus exprimé par celle-ci de son vivant.

Publicité des décisions – Aux termes de l'article 46, « la formation restreinte peut rendre publiques les sanctions qu'elle prononce. Elle peut également ordonner leur insertion dans des publications, journaux et supports qu'elle désigne aux frais des personnes sanctionnées. Le président de la commission peut demander au bureau de rendre publique la mise en demeure prévue au deuxième alinéa du I de l'article 45[390]. Lorsque le président de la commission prononce la clôture de la procédure dans les conditions définies au troisième alinéa du même I, la clôture fait l'objet de la même mesure de publicité que celle, le cas échéant, de la mise en demeure »[391]. Toutes les décisions prises par la CNIL sont donc susceptibles de publicité, mises en demeure comprises, même si cette mesure demeure exceptionnelle. Une telle diffusion[392] ne constitue pas une entrave au droit pour le responsable de traitement de contester les décisions de la CNIL[393]. La publicité constitue une sanction souvent efficace pour certaines sociétés, attachées à leur image de marque[394]. Au-delà, elles ont un effet prophylactique. Les utilisateurs sont alertés des risques d'atteinte à leurs droits qu'ils encourent. A cette fin, encore faut-il s'assurer de la diffusion satisfaisante de ces condamnations tant dans l'espace que dans le temps. Une simple publication sur le site Internet de la CNIL peut s'avérer insuffisant. Il en va de même d'une communication de quelques heures seulement.

L'éventuel avenir – Les instances européennes partagent avec le droit français le souci de soutenir le contrôle administratif *a posteriori*. Ce contrôle est agencé par les articles 46 et suivants de la proposition de règlement. Certaines mesures devraient accentuer ce contrôle. Ainsi, la proposition prône la consécration d'un principe de cohérence entre les diverses autorités de contrôle des états membres. Celles-ci veillent à l'application uniforme du règlement dans les Etats membres, sous le contrôle du comité européen de la protection des données[395]. Cette uniformisation est naturellement pertinente, à condition qu'elles assurent une

[390] Délib. CNIL 2013-217 du 17 juillet 2013 décidant de rendre publique la mise en demeure n° 2013-029 du 12 juillet 2013 à l'encontre de la société BRESSE DIS exploitant l'enseigne « E. Leclerc ».
[391] Pour des applications : CNIL, délib. n∞ 2010-113, 22 avr. 2010. - CNIL, communiqué, La CNIL adresse un avertissement à ACADOMIA pour des commentaires excessifs dans ses fichiers, 27 mai 2010 : www.CNIL.fr.
[392] Délib. CNIL n° 2014-014, décidant de rendre publique la mise en demeure n° 2014-001 du 15 janvier 2014 prise à l'encontre de la société HYPERCOSMOS exploitant l'enseigne « E. LECLERC ».
[393] CE., ord. réf. 7 février 2014, n° 374595, Jurisdata n° 2014-001914 ; Comm. com. électr. 2014, comm. 29, A. Lepage **:** rejet de la requête de la société Google visant à obtenir la suspension de la publication de la décision de la CNIL du 3 janvier 2014.
[394] Voir ainsi « l'affaire Google ». L'entreprise GOOGLE a saisi le Conseil d'état d'une requête contre la délibération de la CNIL n° 2013-420 du 3 janv. 2014 la CNIL qui prononce une sanction pécuniaire de 150 000 euros. Celle-ci se cumulait avec l'obligation de publier cette décision publique sur le site de la CNIL et celle de faire paraître sur son site Internet *www.google.fr*, pendant une durée de 48 heures consécutives un communiqué relatif à la sanction prise à son encontre pour manquements aux règles de protection des données personnelles. La société a refusé de déférer à cette décision.
[395] Pour un renforcement des pouvoirs de cette nouvelle autorité : N. Martial-Braz, *op. cit*., p. 15 et s.

protection vers le haut, en contraignant les états dans lesquels les surveillances sont moins poussées à s'aligner sur les états précurseurs en ce domaine. En outre, on peut craindre que la stratification des instances de contrôles n'alourdissent et de ce fait ne ralentissent les vérifications. Chaque autorité nationale doit pouvoir agir avec le plus d'indépendance possible.

Les fonctions de ces autorités de contrôles sont celles dont disposent déjà la CNIL[396]. Quant aux sanctions, un ordonnancement précis est posé. La proposition de règlement semble instituer une hiérarchie de ces dernières, avec au sommet les sanctions financières. Concernant ces dernières, le montant de la condamnation était fonction de la gravité de la faute. La violation du droit à l'oubli numérique de propos délibérés ou par négligence devait donner lieu à une amende de 500.000 euros ou pour les entreprises à 1 % du chiffre d'affaires mondial[397]. Une faute non intentionnelle ne donnait lieu qu'à un avertissement. Le Parlement européen propose cependant d'en revenir à un système plus classique, tout en apportant des innovations intéressantes. Le responsable encourt au moins l'une des sanctions suivantes : un avertissement, des vérifications périodiques régulières de la protection des données, une amende pouvant atteindre 100 000 000 euros ou 5 % du chiffre d'affaires annuel mondial s'agissant des entreprises. L'autorité de contrôle peut opter pour une amende supérieure au pourcentage du chiffre d'affaires si elle le souhaite, dans la limite de 100 000 000 euros. L'avertissement semble cantonné aux infractions non intentionnelles. Si le responsable de traitement est détenteur d'un label européen de protection des données, il ne sera sanctionné qu'en cas d'infraction délibérée ou par négligence. Une liste des critères d'appréciation de la sanction adéquate est livrée par l'article 79, 2 quater. Y figurent notamment la nature, la gravité et la durée de la non-conformité, le caractère répétitif de l'infraction, les catégories de données affectées, la gravité du dommage, les mesures prises pour atténuer ce dernier, les avantages financiers escomptés et les pertes évitées, le refus ou on de coopérer au contrôle…

Le Parlement paraît plus réticent en revanche sur la publicité des délibérations des autorités de contrôle. S'il confirme cette faculté, il propose toutefois d'indiquer expressément que des « mécanismes de notification confidentiels soient également mis en place »[398].

Enfin, on relèvera un élargissement des facultés de saisine de l'autorité de contrôle. L'article 73 reconnaît en effet ce droit aux associations, organismes ou organisation qui

[396] Articles 52 et suivants du projet de règlement.
[397] Article 79, 5 c du projet de règlement.
[398] Article 53 bis j nouveau de la résolution du Parlement européen.

« œuvrent à la défense des intérêts des personnes concernées à l'égard de la protection de leurs données », s'ils observent une violation de ces droits, peu importe que leurs actions soutiennent ou non une ou plusieurs réclamations individuelles. Dans sa résolution, le Parlement recadre ce droit aux associations qui défendent « l'intérêt public ». On peut regretter la généralité des termes de ces dispositions, qui devront être précisés par les législations nationales de transposition.

2.3.2.2. La responsabilité civile

Alors que la directive de 1995 et la proposition de règlement européen encouragent les Etats membres à mettre en place un système de responsabilité ou plus précisément de réparation aux victimes, la loi de 1978 demeure peu prolixe sur cette sanction. L'article 22 du projet de règlement garantit ainsi le droit à un recours juridictionnel indépendamment de tout recours administratif. En droit français, à défaut de disposition spécifique, le droit commun de la responsabilité s'applique. L'intéressé qui se heurterait à une violation de son droit à l'oubli devrait alors faire état d'un fait générateur de responsabilité et d'un préjudice en lien causal avec ce dernier, conditions peu évidentes à caractériser.

La faute, fait générateur - Plusieurs questions doivent être résolues : la nature de la faute d'une part, la charge de la preuve d'autre part, la responsabilité du sous-traitant enfin.

Responsabilité contractuelle ou délictuelle – Deux analyses sont envisageables sur la nature de la responsabilité.

Selon une première analyse, lorsque la loi exige que l'intéressé donne son consentement au traitement de ses données personnelles, on peut supposer qu'un contrat se forme entre les protagonistes. Il s'agirait d'un contrat *sui generis* autorisant le responsable à faire usage des données dans une finalité définie. Dans ce cas, l'inobservation des dispositions légales relèverait de la responsabilité contractuelle. Une telle qualification inviterait à s'interroger sur la mesure de l'autonomie des contractants. On devrait postuler que les droits de retrait, de rectification ou d'opposition sont d'ordre public et qu'ils ne donnent aucune prise à la liberté contractuelle sur leur principe. Tout au plus, les parties seraient libres d'en aménager les modalités de mise en œuvre, à condition que celles-ci ne soient pas trop contraignantes pour l'utilisateur.

Selon une seconde analyse, on peut estimer que les obligations du responsable de traitement ont une nature exclusivement légale. Partant, que la personne consente ou non à l'opération, la responsabilité demeurera délictuelle. On exprimera une préférence pour cette analyse. La protection des données personnelles ne doit pas donner prise à la volonté des intéressés. Toute clause limitative de responsabilité ou clause de compétence serait de la sorte prohibée. Le statut légal devrait l'emporter sur l'autonomie contractuelle.

Le fait générateur de responsabilité – A défaut de régime spécifique de responsabilité de plein droit, la responsabilité du responsable de traitement est conditionnée à sa faute. Celle-ci sera caractérisée toutes les fois où le responsable du traitement refusera d'obtempérer à la demande de l'intéressé de retirer ou de supprimer une donnée. Elle sera également avérée si la donnée est conservée pour une durée supérieure à celle requise par la finalité du traitement.

Le projet de règlement et la résolution de la commission adoptent cette conception extensive de la faute. Ainsi l'article 77 précise que « toute personne ayant subi un dommage du fait d'un traitement illicite ou de toute action incompatible avec le présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi ». La résolution législative sur ce projet de règlement propose de substituer à l'expression « la victime a le droit d'obtenir », l'assertion « la victime a le droit d'exiger ». Ce changement terminologique vise à accentuer le caractère obligatoire de la sanction. Il n'en demeure pas moins que juridiquement, la mutation est insensible. Dès lors que les conditions de la responsabilité sont réunies, la victime est en droit d'être indemnisée. Il vaudrait d'ailleurs mieux qu'elle obtienne réparation sans l'exiger, qu'elle ne l'exige sans l'obtenir.

Responsabilité des tiers dans le projet de règlement – Cette question est envisagée spécifiquement par la proposition de règlement. Ainsi le sous-traitant est considéré comme un débiteur potentiel d'indemnisation, au même titre que le responsable de traitement. La victime peut obtenir la condamnation *in solidum* de ces deux protagonistes[399].

Toutefois considérant plus spécifiquement le droit à l'oubli, l'article 17 §2 dispose que si le responsable de traitement « a autorisé un tiers à publier des données à caractère personnel, il est réputé responsable de cette publication »[400]. Cette responsabilité du fait d'autrui disparait

[399] Art 77 du projet de règlement.
[400] Sur cette question, voir N. Martial_Braz (sous la resp.), *op. cit*., p. 35 et s.

dans la résolution du Parlement européen. Néanmoins, le sous-traitant devrait demeurer un responsable à titre personnel sur le fondement de la disposition précédente.

Charge de la preuve – La détermination de la personne sur qui pèse le fardeau probatoire est essentielle. A défaut de pouvoir bénéficier d'un régime de responsabilité sans faute, les utilisateurs dont les droits ont été lésés doivent pouvoir escompter sur un régime de preuve qui leur soit favorable. Cet allègement se justifie d'autant plus qu'ils seront souvent impuissants à démontrer la faute. Les responsables de traitement seront mieux positionnées pour établir qu'ils se sont ou non conformés aux obligations légales. L'article 40, alinéa 2 de la loi de 1978 abonde en ce sens. Il opère un renversement de la charge de la preuve. Lorsqu'une personne le demande, le responsable de traitement doit pouvoir justifier avoir satisfait à l'exigence de retrait ou de modification du traitement. De même, l'alinéa 3 de cet article dispose, à propos du droit d'accès, qu'« en cas de contestation, la charge de la preuve incombe au responsable auprès duquel est exercé le droit d'accès sauf lorsqu'il est établi que les données contestées ont été communiquées par l'intéressé ou avec son accord ». Une même règle pourrait être exprimée explicitement pour le droit à l'oubli. La preuve de la mise en œuvre de ce droit ne peut en effet être utilement rapportée que par le responsable du traitement. S'il échoue, la faute sera caractérisée et la victime indemnisée à hauteur de son préjudice.

Une telle disposition ne se retrouve pas dans la proposition de règlement. L'alinéa 3 de l'article 77 se contente de préciser que le responsable du traitement ou le sous-traitant peut s'exonérer de sa responsabilité s'il prouve que le fait invoqué ne lui est pas imputable, *i.e.* soit son absence de faute, soit l'absence de lien causal entre le fait générateur et le préjudice allégué. Aussi doit-on en inférer que la preuve doit au préalable être rapportée par la personne dont les données ont été traitées.

Le préjudice et la causalité, conditions dissuasives - En droit commun, la preuve d'un préjudice en lien causal avec la faute est une condition *sine qua non* de la responsabilité. En son absence, le demandeur devra être débouté. Cette condition constituera certainement le principal obstacle à l'efficience du droit de la responsabilité à garantir un droit à l'oubli.

Il n'est pas neutre à cet égard que la résolution ressente le besoin de préciser que le préjudice extrapatrimonial est également réparable. Cet ajout est important dans certains droits plutôt réticents à l'admettre. Il l'est aussi dans les droits qui le reconnaissent, comme le droit français, car souvent seul cet intérêt de l'utilisateur sera lésé. Il faut également entendre par

cette assertion que le droit à réparation de la victime est bien fondé alors même qu'elle ne revendiquerait qu'un préjudice de cet ordre, avec toute la difficulté inhérente à son appréhension et à son évaluation.

Hormis cette précision, les divers textes étudiés restent muets sur la question du préjudice. Tout au plus, l'alinéa 4 de l'article 40 énonce-t-il que «lorsqu'il obtient une modification de l'enregistrement, l'intéressé est en droit d'obtenir le remboursement des frais correspondant au coût de la copie mentionnée au I de l'article 39 ».

Au-delà des sanctions financières, l'intérêt de l'utilisateur est essentiellement d'obtenir en justice des mesures de réparation en nature, comme l'effacement sous astreinte des données litigieuses, la publicité de la condamnation, voire l'interdiction à l'avenir de tout traitement.

En somme, le préjudice dont la réparation sera demandée se résumera, dans la plupart des cas, à un préjudice moral, dont l'étendue sera souvent réduite. Une action en justice pourra aussi être motivée par la volonté de contraindre un responsable récalcitrant à effacer les données demandées. Le juge pourra l'y forcer notamment sous la menace d'astreinte. Cette mesure de réparation n'est pas exclusive de la réparation en équivalent si la première n'est pas de nature à effacer la totalité du dommage subi par la victime.

Le droit positif de la responsabilité civile et la réforme éventuelle à venir ne paraissent guère contraignants pour le responsable du traitement qui, économiquement, tirera peut-être plus avantage à la violation de la loi qu'à son respect. Les personnes dont les droits ont été lésés risquent d'être dissuadées d'ester en justice soit parce que la procédure est longue et couteuse, soit parce que l'issue est insatisfaisante. De fait, si le nombre de plaintes auprès de la CNIL ne cesse d'augmenter chaque année, le contentieux reste assez réduit.

Palliatifs - Plusieurs voies pourraient être explorées pour remédier à ces faiblesses de notre droit.

Présomption du préjudice – Une présomption de préjudice, comme le droit français en connait déjà en droit de la concurrence ou au sujet de la vie privée, pourrait être consacrée. Le dommage se déduirait nécessairement de la faute et son quantum serait laissé à la souveraineté des juges du fond. Une méthode de calcul indicative pourrait être instituée comme pour la contrefaçon. Les dommages intérêts pourraient notamment tenir compte de la gravité

de la faute et des profits retirés du manquement par le responsable du traitement. Un tel résultat pourrait être obtenu, si le droit à l'oubli était confondu avec l'atteinte à la vie privée. On appliquerait au premier le régime de la seconde. On pourrait y parvenir également en érigeant le droit à l'oubli en un véritable droit subjectif, dont la violation serait sujette à sanction[401]. Ce droit serait assorti d'un contenu et d'un régime autonomes. Il conviendrait également de le situer dans la hiérarchie des normes et d'échafauder son articulation avec d'autres droits fondamentaux. La proposition de règlement semblait cheminer en ce sens. La proposition de résolution semble faire marche arrière puisque le terme de droit à l'oubli a disparu au profit de celui, moins engageant, d'effacement[402]. Des dommages et intérêt punitifs sanctionnant une faute, plus que réparant un dommage, pourraient encore être envisagés.

Actions collectives – La consécration d'actions de groupe pourrait également constituer un moyen pertinent pour assurer la protection de la législation sur les données personnelles. Un particulier serait certainement moins réticent à agir s'il unissait ses forces à celles d'autres personnes lésées. De surcroît, cette dimension collective est déterminante lorsque pour un opérateur économique ce n'est pas la collecte d'une donnée qui est lucrative mais la constitution d'une base significative qu'il pourra exploiter. Une action d'un ensemble de personnes concernées par cette base aura certainement plus d'efficacité. La loi dite Hamon du 17 mars 2014 a introduit ce type d'action en droit français. Le domaine de cette dernière demeure cependant doublement limité. Quant à son objet, elle est réservée aux manquements légaux ou contractuels des professionnels à l'occasion de la vente de biens ou de la fourniture de services. Quant au préjudice appréhendé, elle ne peut permettre la réparation que des seuls préjudices patrimoniaux résultant de dommages matériels subis par les consommateurs[403]. Sortent donc de son champ d'application les préjudices extrapatrimoniaux. En encourageant les associations à agir, les instances communautaires ne semblent pas hostiles à ce type d'action, même si les dispositions qu'elles y consacrent demeurent assez vagues sur les contours de leurs missions et de leurs moyens d'actions. Ce flou peut être analysé par les Etats comme une brèche dans laquelle le législateur pourrait s'engouffrer pour consacrer une action de groupe ou pour élargir son domaine concernant les pays qui en connaissent déjà.

[401] Adde : N. Martial-Braz (sous la dir), *op. cit*., n° 45 : « la consécration d'un véritable droit à l'oubli numérique supposerait (…) des mesures permettant la remise en cause de traitements licites ».
[402] Article 17 du projet de règlement.
[403] Pour les premiers commentaires, voir notamment : V. Rebeyrol, » La nouvelle action de groupe », D. 2014, chron. 940 ; N. Molfessis, « L'exorbitance de l'action de groupe à la française », D. 2014, chron. 947.

En conclusion de cette troisième partie, il y a eu lieu de considérer que même envisagé *a minima*, un droit à l'oubli est complexe dans sa mise en œuvre.

Les techniques de sécurisation des données disponibles à ce jour n'étant pas totalement fiables, elles laissent planer un doute quant à la possibilité de garantir aux usagers un contrôle de la circulation des données et, par voie de conséquence, un droit à l'oubli effectif. En outre, même si une solution technique efficace et générique existait, elle ne pourrait avoir de sens que si les utilisateurs avaient confiance dans son efficacité.

La construction d'une confiance du public dans une technologie est un problème qui ne peut pas se résoudre uniquement avec des outils techniques, informatiques et mathématiques. En effet, il s'agit d'un problème essentiellement humain qui porte en lui les germes d'un autre risque : celui, au final, d'avoir réussi à établir une confiance du public dans un système qui, techniquement, ne le mérite pas, car présentant trop de failles et de défauts. Ce dernier risque peut sembler suffisamment menaçant pour qu'en définitive, l'absence de solution technique généralisable à toute situation paraisse finalement quelque peu rassurante.

La sécurité des personnes concernées sera donc confortée par une *information pertinente*. Cette information est destinée, de façon préventive, à permettre à chacun de mesurer les conséquences de la diffusion, par elle-même, de certaines informations au public. Une démarche en ce sens est engagée dans le projet de loi tendant à moderniser la loi de 1978[404]. L'article 1er prévoit d'ajouter au Code de l'éducation un alinéa qui intègre au programme d'éducation civique un enseignement « sur les risques liés aux usages des services de communication au public en ligne ». L'enquête sociologique avait d'ailleurs révélé que les jeunes adultes n'avaient pas bénéficié d'enseignements spécifiques sur la question mais que leur frère et/ou sœur plus jeunes en avaient suivis dans le cadre d'actions de sensibilisation menées dans leur école. C'est un point qu'il ne faut pas négliger.

Les limites techniques ne doivent cependant pas conduire à renoncer à l'idée d'un droit à l'oubli car s'il est impossible de garantir de manière absolue un effacement ou un déréférencement définitif, dans la très grande majorité des cas, les techniques disponibles suffiront à satisfaire les demandes.

C'est pourquoi le mouvement amorcé par les instances européennes doit être soutenu. Le cadre de la protection des données personnelles est en effet suffisamment souple pour couvrir la problématique du droit à l'oubli et le recours à un règlement doit être approuvé en raison de l'effet uniforme qu'il procure sur le territoire de l'Union européenne. Les initiatives des opérateurs pour l'adoption de chartes ne doivent pas faire illusion. Elles comportent pour

[404] Proposition de loi adoptée par le sénat le 6 nov. 2009 (sénat n° 93), transmise à l'AN en 1ère lecture le 24 mars 2011 (A.N. n°2387).

les usagers, un risque intrinsèque car leur portée juridique est faible ce qui résulte notamment de l'aléa lié à la sanction de leur violation et, un risque extrinsèque car cela conduit à une multiplication des sources au sein desquels l'usager risque de se perdre. Il convient donc de privilégier le cadre juridique de la protection des données à caractère personnel, ce qui inclut les sanctions qu'il prévoit.

CONCLUSION GENERALE

Le droit à l'oubli est une idée séduisante mais la nécessité de consacrer un droit à l'oubli autonome ne nous semble pas si évidente. La question du droit à l'oubli numérique est certes l'un des enjeux majeurs de la protection des citoyens et du respect du droit à la vie privée, voire de l'existence d'un droit à l'erreur et de la possibilité de se racheter ou plus simplement, d'un droit à la tranquillité.

Néanmoins, le droit à l'oubli existe déjà, du moins implicitement. La loi informatique et libertés, la loi pour la confiance dans l'économie numérique, le droit au respect de la vie privée, sans le prévoir explicitement, comportent des prérogatives y conduisant. La jurisprudence tant française qu'européenne a su s'en accommoder et répondre aux cas critiques. Ces différents dispositifs demeurent, malgré les évolutions du numérique et la très grande accessibilité à Internet, des textes de large portée. C'est vrai tout particulièrement de la loi Informatique et libertés eu égard à la définition de son champ d'application que ce soit au regard de la notion de données à caractère personnel, de traitement ou de responsable de traitement. Elle est susceptible de couvrir de larges champs et d'offrir aux individus une protection pertinente, l'arrêt rendu par la CJUE le 13 mai 2014 l'atteste.

Précisément, cette décision est déterminante au regard du concept de droit à l'oubli car elle met le doigt sur ce qui, de notre point de vue, constitue la spécificité du droit à l'oubli par rapport au droit à la protection des données personnelles en général.

Premièrement, qu'il s'agisse du numérique ou non, les demandes judiciaires tendant à bénéficier d'un droit à l'oubli sont toujours liées à *la diffusion* d'une information concernant une personne. C'est le fait de *rendre publique* une information qui se trouve donc au cœur de la problématique du droit à l'oubli. On rappellera que le régime de protection des données personnelles couvre bien la diffusion en ce qu'elle constitue un traitement de données.

Deuxièmement, à notre avis, créer un droit à l'oubli n'aurait de sens et d'intérêt que s'il s'agit de lutter contre la diffusion d'un *contenu licite*. En effet, la victime d'une diffusion de contenus illicites est protégée par d'autres prérogatives qui ont fait la preuve de leur efficacité. Le droit à l'honneur et à l'intégrité morale (et l'action en diffamation), les droits de propriété intellectuelle (et l'action en contrefaçon), le droit au respect de la vie privée (et l'action en responsabilité délictuelle) ou encore, le droit à la protection des données personnelles (par le droit de rectification ou d'opposition par exemple).

On constate toutefois que ce dernier dispositif ne distingue pas selon le caractère licite ou non des données. C'est là tout son intérêt au regard de la problématique du droit à l'oubli. Il apparaît donc bien comme un instrument juridique capable d'offrir un droit à l'oubli.

Troisièmement, toujours dans cette volonté d'identifier la spécificité du droit à l'oubli, l'intérêt de consacrer un tel droit était étroitement lié à la possibilité d'obtenir par ce biais, une prérogative permettant de s'opposer à tout type de traitement, y compris donc, *aux traitements a priori licites des données*. En effet, si le droit à l'oubli s'appliquait uniquement aux traitements illicites, tels que définis par le droit positif en vigueur, qu'apporterait-il de nouveau ? Ce critère peut effrayer de prime abord. Si le droit à l'oubli s'appliquait aux traitements licites, l'individu reprendrait la maîtrise de tout type de traitement possible et imaginable. En réalité, d'une part, le traitement dont il est question serait un traitement licite au départ mais qui devient illicite parce qu'il n'est pas (plus) conforme à la volonté de la personne concernée et qu'aucune obligation légale n'impose leur traitement. Il ne s'agit pas là d'une hypothèse nouvelle à ceci près que la volonté de l'individu de ne plus permettre le traitement d'une donnée est aujourd'hui enfermée dans des limites strictes qu'il conviendrait d'assouplir avec une mise en balance des différents droits en présence – spécialement droit à l'oubli d'un côté et liberté d'expression et droit à l'information de l'autre – sans préjuger de celui qui l'emporte, puisque, jusqu'à la décision Google Spain c/ AEPD, la mise en balance conduisait à privilégier le droit à l'information – . D'autre part, si l'on reprend la première caractéristique du droit à l'oubli décrite ci-dessus, cette crainte ne se justifie plus. L'un des objectifs principaux du droit à l'oubli vise à permettre aux usagers de s'opposer à la diffusion. Il peut venir au soutien du droit à l'effacement, comme par exemple, l'effacement réel des données laissées sur les réseaux sociaux, mais le droit à l'oubli ne saurait se résumer à un droit à l'effacement des données. Il en résulte qu'une donnée personnelle qui a été traitée licitement par un opérateur pourrait, au bout d'un certain temps, justifier la mise en œuvre du droit à l'oubli qui consisterait à ne plus permettre pour l'avenir de lier la personne concernée à cette donnée sans que cette dernière soit effacée.

Il reste alors à identifier l'opérateur qui décide du sort des données ? D'un point de vue juridique et technique, il convient d'être réservé quant à la possibilité de créer un droit à l'oubli numérique à la charge des moteurs de recherche car cela conduirait à demander aux moteurs de recherche d'agir au cas par cas sur des contenus dont ils n'ont pas nécessairement la maîtrise. Dans la mesure où la décision implique de déterminer d'abord la nature licite ou illicite du contenu, il conviendrait d'organiser un mécanisme de subsidiarité. Au premier chef, seraient

visés les auteurs et/ou les éditeurs[405]. A titre subsidiaire, si ces derniers s'abritaient derrière le caractère licite du contenu pour refuser de l'effacer, l'usager devrait saisir une autorité indépendante de contrôle – en France, la CNIL – qui se prononcerait sur le bienfondé de la demande de déréférencement. Dans l'hypothèse où l'usager ne contesterait pas le caractère licite de l'information le concernant, il pourrait s'adresser directement à la CNIL en vue d'un déréférencement par le moteur de recherche.

Les conclusions rendues par l'avocat général dans l'affaire Google Spain C/ AEPD pouvaient laisser à penser que le droit positif ne permettait pas la mise en œuvre d'une telle solution sans la création d'un droit à l'oubli autonome. La décision rendue par la CJUE, à revers de ces conclusions, a montré au contraire que la directive de 1995 permettait d'offrir cette protection aux individus. Si le règlement pour la protection des données personnelles est adopté, la solution sera encore plus nette puisque l'article 17 permet le déréférencement qu'il dissocie bien de l'effacement des données.

Il s'ensuit que le dispositif de protection des données à caractère personnel, par sa portée et les dispositifs de mise en œuvre qu'il propose nous parait répondre de manière satisfaisante à la problématique du droit à l'oubli qu'il n'y a pas lieu d'ériger au rang de droit subjectif autonome. Ainsi que nous le soulignions en conclusion de la deuxième partie, dans cette approche, le droit à l'oubli doit être envisagé comme un concept générique couvrant différents dispositifs techniques et juridiques concourant à la protection de la personne à travers ses données et dont la mise en œuvre favorise la tranquillité de la personne et limite les intrusions malsaines dans sa vie.

D'un point de vue formel, mais non dépourvu de conséquences au fond, le législateur pourrait consacrer le droit à l'oubli dans une disposition générale introductive qui érigerait le droit à l'oubli au rang des fondements de la protection des données à caractère personnel.

[405] En ce sens, Conseil d'Etat, « Le numérique et les droit fondamentaux », Les rapports du Conseil d'Etat, sept. 2014, p. 188.

BIBLIOGRAPHIE

Rapports et délibérations de la CNIL

- CNIL Rapports d'activité (annuels)
- CNIL Délib. n°2011-238 CNIL
- CNIL Délib. n°1985-44 du 15 octobre 1985.
- CNIL Délib. n°2000-064 du 19 décembre 2000
- CNIL Délib. n°2001-057 du 29 novembre 2001
- CNIL Délib. n°2005-002, 13 janvier 2005.
- CNIL Délib. n°2005-284, 22 novembre 2005
- CNIL Délib. n°2006-102 du 27 avril 2006
- CNIL Délib. n°2010-072, 18 mars 2010.
- CNIL Délib. n°2010-113, 22 avr. 2010
- CNIL Délib. n°2010-232, 17 juin 2010
- CNIL Délib. n°2011-204 du 7 juillet 2011
- CNIL Délib. n°2012-320, 20 septembre 2012
- CNIL Délib. n°2012-475 du 3 janvier 2013
- CNIL Délib. n°2013-173 du 19 juin 2013
- CNIL Délib. n°2013-217 du 17 juillet 2013
- CNIL Délib. n° 2014-014 du 16 janvier 2014
- CNIL Délib. n°2005-188 du 8 septembre

Avis du Groupe de travail « article 29 » sur la protection des données

- Avis 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche du 4 avril 2008.
- Avis 5/2009 sur les réseaux sociaux en ligne du 12 juin 2009.
- Avis 15/2011 sur la définition du consentement du 13 juillet 2011.

Ouvrages et rapports

- Anderson R., *Trusted Computing frequently asked questions*, 2003 (http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html).
- Belleil A, *E-privacy : le marché des données personnelles : protection de la vie privée à l'âge d'Internet*, Dunod, 2001.
- Bensoussan A. et Türk A., *Informatique et libertés*, Ed. Francis Lefèvre, 2010, 2è éd. 2010, 955 p.

- Bergson H., *L'Energie spirituelle. Essais et conférences* (1919), P.U.F., 2009, Chapitre I, p.34.
- Bras P.-L, *Rapport sur la gouvernance et l'utilisation des données de santé*, remis à la Ministre des affaires sociales et de la santé en septembre 2013.
- Carbonnier J., *Droit civil, introduction*, PUF 1ère éd. 1955, rééd. en 2004.
- Carbonnier J., *Droit des obligations*, PUF, pp. 627-628
- Casassa Mont M., Pearson S. & Bramhall P., *Towards accountable management of identity and privacy: sticky policies and enforceable tracing services*, Rapport de recherche HP labs HPL-2003-49, Royaume-Uni, 2003.
- Collin P., Colin N., *Mission d'expertise sur la fiscalité du numérique,* Rapport au Ministre de l'économie et des finances, au Ministre du redressement productif, au Ministre chargé du budget, à la Ministre déléguée chargée des petites et moyennes entreprises, de l'innovation et de l'économie numérique, janvier 2013.
- Comité consultatif Google, *The advisory council to Google on the right to be forgotten*, 6 février 2015.
- Conseil d'Etat, *Internet et les réseaux numériques*, Doc. fr., 2000, p. 186.
- Conseil d'Etat, *Le numérique et les droit fondamentaux*, Les rapports du Conseil d'Etat, septembre 2014.
- Conseil économique et social des Nations Unies, *Sociétés transnationales : l'élaboration d'un code de conduite et les questions qu'elle soulève*, Rapport du secrétariat, New-York, ONU, 1976, p.12.
- Danet J., *La justice pénale entre rituel et management*, PUR 2010.
- Desgens-Pasanau G., *La protection des données à caractère personnel*, LexisNexis, 2012.
- Desportes F. et Le Gunehec F., *Droit pénal général*, Economica, 16e éd., 2009
- Doris S., *A Peer-to-peer Infrastructure for Social Networks,* thèse de doctorat, TU Berlin, 2008.
- Ferenczi T., *Devoir de mémoire, Droit à l'oubli* ? Ed. complexe, 2002.
- Forum des droits de l'Internet, *Quelle responsabilité pour les créateurs d'hyperliens vers des contenus illicites ?* : Recomm. rendue publique, 23 oct. 2003.
- Gutmann D., *Le sentiment d'identité*, Préf. F. Terré, LGDJ, 2000 Ho A. T., *Towards a Privacy-Enhanced Social Networking Site*, Thèse de doctorat, Université de Montréal, 2012.
- LIBE (Commission) Rapport du 21 octobre 2013 de la commission des libertés civiles, de la justice et des affaires intérieures, A7-0403/2013.
- Malaurie P. et Morvan P., *Droit civil, Introduction générale*, Defrénois 2013.
- Manara C., Les réseaux sociaux : 101 questions juridiques, éd. Diateno 2014.
- Mayer-Schönberger V., *Delete: The virtue of forgetting in the digital age*, 2009, Princeton university press.
- Morin-Desailly C., *L'Europe au secours de l'Internet : démocratiser la gouvernance de l'Internet en s'appuyant sur une ambition politique et industrielle européenne*, Rapport

d'information n° 696 (2013-2014) sur la gouvernance mondiale de l'Internet, déposé le 8 juillet 2014.

- Nietzsche F., *Considérations intempestives*, II, 1, 1874 tr. fr. G. Bianquis, éd. Aubier-Montaigne.
- Nietzsche F., *Généalogie de la morale*, Flammarion, 1996.
- OCDE, *Les codes de conduite des entreprises – Etude approfondie de leur contenu, Paris,* OCDE, 2000.
- Perri P., Google, un ami qui ne vous veut pas que du bien, éd. Anne Carrière, 2013.
- Quillet E, *Le droit à l'oubli numérique sur les réseaux sociaux*, mémoire de master de droits de l'homme et droits humanitaire, dir. E. Decaux, 2011.
- Ricoeur P., *La mémoire, l'histoire, l'oubli*, Le Seuil, 2000.
- Robert J.-H., *Droit pénal général*, PUF, coll. Thémis, 6e éd., 2005, p. 543.
- Rochfeld J., *Les grandes notions du droit privé*, PUF, Thémis droit, 2011.
- Rosa H., *Accélération*, La découverte, 2010.
- Sueur J.P., *Numérique, renseignement et vie privée : de nouveaux défis pour le droit*, Rapport d'information sénat, n° 666, 27 juin 2014.

Articles

- Aubert M., Broussy E., Cassagnabere H., « Vie privée et protection des données personnelles – Moteur de recherche et droit à l'oubli » AJDA 2014, p.1147.
- Ayrault L., « Droit fiscal européen des droits de l'homme : chronique de l'année 2013 », à propos de CEDH 14 mars 2013, Rev droit fiscal, n° 10, mars 2014, n°201.
- Backes J., Backes M., Dürmuth M., Gerling S. & Lorenz S., X-pire!: « An expiration date for images in social networks », 2011 (http://arxiv.org/abs/1112.2649).
- Bailly E. et Le Corre C., « L'entreprise et la protection des données personnelles, Revue Lamy Droit des affaires », 2013, n°87.
- Barrau L. et Tessonneau A., « Protection des données personnelles et risques juridiques pour l'entreprise », Economie et Management, n°147, Avril 2013, p. 24.
- Beignier, « Vie privée et vie publique », Légipresse sept. 1995, p. 67 s..
- Bellivier F. et Noiville C., « Code de conduite et équité des échanges de ressources biologiques », Idées pour le débat, n°10, 2006, p.7, http://www.iddri.org.
- Benabou V. et Rochfeld J., « Les moteurs de recherche, maîtres ou esclaves du droit à l'oubli numérique ? Acte I : le moteur, facilitateur d'accès, agrégateur d'informations et responsable de traitement autonome », Dalloz 2014 p.1476.
- Berguig V.-M. et Thiérache C., « L'oubli numérique est-il de droit face à une mémoire numérique illimitée ? », Cyberlex, rapport du 25 mai 2010, Revue Lamy Droit de l'Immatériel 2010 – n°62.

- Bettati V.M., « Réflexion sur la portée du Code international de conduite pour le transfert de technologies : éloge de l'ambiguïté », *in Droit et Liberté à la fin du XX*è *siècle,* Etudes offertes à C.-A. Colliard, Pédone, 1984, p. 83 et suiv..
- Blandin A. et Juet E., « La prévention des risques professionnels à la lumière de la loi informatiques et libertés : le cas du dispositif S_Pod », colloque *Innovations technologiques dans le contexte professionnel*, MSHB, 26 et 27 juin 2014.
- Boizard M. « Détermination de la qualité d'hébergeur : voyage en eaux troubles », Revue Lamy Droit Civil 2013, p. 18.
- Boizard M. « La responsabilité des fournisseurs d'Internet », LAMY Responsabilité, Étude 420, 2012.
- Boizard M., « La responsabilité en matière d'Internet », Revue Droit et patrimoine 2001, n°89, p. 70 s..
- Boizard M., « Les codes de conduite privés, un instrument volontaire juridiquement efficace ? » *in Les approches volontaires et le droit de l'environnement, actes du colloque*, sous la direction de N. Hervé-Fournereau, Préface de Stavos Dimas, PUR 2008, p. 147 s..
- Bossi J., « Comment organiser aujourd'hui la protection des données de santé », RDSS 201, p. 208.
- Bourcier D., de Filippi P., « L'Open Data : l'universalité de principe et diversité des expériences », JCA éd. A, 2013, n° 38, 2260.
- Boy L., « L'éco-label communautaire, un exemple de droit postmoderne », Rev. int. dr. éco., 1996, p. 69.
- Boyer J., « Droit à l'oubli, droit de suppression, droit de suite : la loi Informatique et libertés doit-elle arbitrer la liberté d'expression ? », Légicom n° 46, 2011/1, p. 77 et s.
- Bruguière J.-M., « Faits et méfaits de la perpétuité dans la propriété littéraire et artistique », Propriété industrielle oct. 2010, dossier 10.
- Bruguière J.M., « Le *droit à* l'oubli numérique, un droit à oublier », D.2014, p.299.
- Bui D., « L'éternité selon Facebook », Le nouvel observateur, 31 oct. 2013, n° 2556, p. 88.
- Caron C., « A propos du conflit entre les œuvres de fiction et la vie privée », D. 2003, p. 1715.
- Caron C., « Certains résultats peuvent avoir été supprimés... », Comm. Comm. Electr. 2014, repère 8.
- A. Casanova et D. Véret, « La consécration d'un droit à l'oubli... principalement pour les anonymes », Revue Lamy Droit de l'Immatériel 2014, dossier spécial, n°106.
- Castets-Renard C., « Google et l'obligation de déréférencer les liens vers les données personnelles ou comment se faire oublier du monde numérique », Revue Lamy Droit de l'Immatériel 2014, dossier spécial, n°106.
- Chéron A., « Affaire Mosley / Google : liberté d'expression, atteinte à la vie privée et droit à l'oubli numérique », D. act. Nov. 2013.
- Claudel E. et Thullier B., « Regard sur le droit mou », Revue de jurisprudence commerciale 2006 n° 1 p. 4.

- Costaz C., « Le droit à l'oubli », Gaz. Pal 1995, p. 961.
- Cutillo L., Molva R.et Strufe T., Safebook A., « Privacy-Preserving Online Social Network Leveraging on Real-Life Trust », IEEE Communication Magazine, pp. 94-101, 2009.
- Cyberlex « L'oubli numérique est-il de droit face à une mémoire numérique illimitée ? » du 25 mai 2010, Colloque organisé par Cyberlex, Revue Lamy Droit de l'Immatériel 2011, n°71.
- De Malafosse G., « De l'inapplicabilité du droit à l'oubli », Les petites affiches n° 183, 12 Septembre 2014.
- de Woot P., « Stratégies des entreprises et données personnelles » in *La protection de la vie privée dans la société de l'information*, P. Tabatoni (dir), Paris, PUF pp.101-219.
- Debet A., « Affaire Google Street View, une sanction exemplaire… mais quelles suites ? », Comm. com. électr. janv. 2012, étude 1.
- Debet A., « Une condamnation attendue : le fonctionnement du STIC jugé contraire au droit au respect de la vie privée ! », Comm. Comm. Electr. 2014, comm. 97.
- Debet A., « L'hébergeur d'un blog est un responsable de traitement au sens de la loi Informatique et Libertés », Comm. com. électr., Avril 2012, comm. 41.
- Derieux E., « Protection des données personnelles et communication au public en ligne, Loi du 6 juillet 1978 relative à l'informatique, aux fichiers et aux libertés et autres textes », Revue Lamy Droit de l'immatériel 2011, n° 68.
- Desmarais P., « Quel régime pour la m-Health », Comm. com. électr. 2013, n° 3, étude 5.
- Farjat G, « Réflexions sur les codes de conduite privés, in le Droit des relations économiques internationales », Etudes offertes à B. Goldman, Litec 1982, p. 48.
- Fenoll-Trousseau M.-P., « Les moteurs de recherche : un piège pour les données à caractère personnel », Comm. com. électr. 2006, étude 3.
- Ferraud-Ciandet N., « L'Union européenne et la télésanté », RTD eur. 2010, p. 537.
- Forest D., « Google et le droit à l'oubli numérique : genèse et anatomie d'une chimère juridique », Revue Lamy Droit de l'Immatériel 2014, dossier spécial, n°106.
- Forgeron J.-F et Bénéat A.- L., « De la santé électronique à l'hôpital numérique », Gaz. Pal. 2009, n° 295, p. 5.
- Fourlon A., « *Toute ressemblance avec des personnages existant ou ayant existé…* est-elle constitutive d'une atteinte aux droits de la personnalité ? » Comm. com. électr. 2007, étude 5.
- Fraysse E., « Facebook, Twitter et le web social, les nouvelles opportunités de business: stratégies, marketing, meilleures pratiques », Agence Kawa, Numilog, 2e éd., 2011.
- Frayssinet J., « L'articulation de la liberté d'expression avec l'article 7 de la loi informatique, fichiers et liberté en cas de violation de la vie privée n'est pas un fusil à deux coups », Revue Lamy Droit de l'immatériel 2009/55, n° 1814.
- Freud S., « Psychonévroses de défense », in *Névrose, Psychose et Perversion*, Paris, P.U.F.

- Geambasu R, Kohno T, Levy A. A. & Levy H. M., « Vanish: Increasing data privacy with self-destructing data », *in Proceedings of the 18th USENIX Security Symposium*, 2009.
- Geffray E., « Projet de règlement sur les données numériques. Quelles conséquences pour les personnes concernées et l'entreprise ? », Revue Lamy Droit civil, 2013, n°100.
- Goupy M., « Etat d'exception », in *Dictionnaire de théorie politique*, V. Bourdeau et R. Merrill (dir.), 2012. http://www.dicopo.fr/spip.php?article131.
- Gouttenoire A., « La famille dans la jurisprudence de la Cour européenne des droits de l'homme », Droit de la famille 2013 n°3.
- Griguer M., « Pharmaciens et e-commerce, nouveau défi », Cah. de l'entrep., n° 1, janv. 2014, prat. 5.
- Haas G.et de Tissot O., « Le paradoxe du droit à l'oubli », Expertises mars 2005, p.105.
- Hassler T., « Réflexions sur le droit à l'oubli appliqué aux images de personnes sur internet », Revue Lamy Droit de l'Immatériel 2014, n°107.
- Hassler T., « Droit de la personnalité : Rediffusion et droit à l'oubli », D. 2007, p. 2829.
- Hocquet-Berg S., « Le dossier médical personnel en questions… », RCA juin 2005, alerte 59.
- Hopt K. J., « Le gouvernement d'entreprise – Expériences allemandes et européennes », Revue des sociétés 2001, n° 1.
- Jacque J.-P., « Protection des données personnelles, Internet et conflits entre droits fondamentaux devant la Cour de justice » RTD Eur. 2014 p.283.
- Jehl J., « Suisse : vers un accès plus facile aux données publiques », JCP 2014, 317.
- Karjoth G. & Schunter M., « A privacy policy model for enterprises *», in 15th IEEE Computer Security Foundations Workshop*, IEEE Computer Society Press, 2002.
- Kossaifi C., « L'oubli peut-il être bénéfique? L'exemple du mythe de Léthé : une fine intuition des Grecs » Revue pluridisciplinaire en sciences de l'homme et de la société ¿ Interrogations ? n°3. L'oubli, déc. 2006.
- Le Clainche J., « CJUE : le droit à l'oubli n'est pas inconditionnel », Revue Lamy Droit de l'immatériel 2014, n° 107.
- Le Clainche J., « Droit des données personnelles et liberté d'expression : hiérarchisation ou conciliation ? » Revue Lamy Droit de l'immatériel 2010/56, n° 1843.
- Lepage A., « La notion de vie privée au sens de l'article 8 de la CEDH ne cesse de prendre de l'ampleur (au sujet de l'aff. Rotaru c/ Roumanie du 4 mai 2000) », D. 2001, p. 1988.
- Lesaulnier F., « L'informatisation des données de santé et la législation Informatique et Libertés », in colloque *Gouvernance et sécurité des systèmes d'information de santé*, Marseille, juin 2001.
- Letteron R., « Le droit à l'oubli », Revue du droit public, 1996, T. CV, n°2, p. 388 note 15.
- Linant de Bellefonds X., « Les hyperliens », Comm. com. électr. 2003, n°5, repères p. 3.
- Marino L., « Les nouveaux territoires des droits de la personnalité », Gazette du Palais 2007, n 139, p. 22.

- Marino L., « Un « droit à l'oubli » numérique consacré par la CJUE », JCP G 2014, p. 768.
- Marino L., « Comment mettre en œuvre le « droit à l'oubli » numérique ? », D. 2014, p. 1680.
- Martial-Braz N. et Rochfeld J., « Les moteurs de recherche, maîtres ou esclaves du droit à l'oubli numérique ? Acte II : le droit à l'oubli numérique, l'éléphant et la vie privée », Dalloz 2014 p.1481.
- Martial-Braz N., « Données de santé », *in La proposition de règlement européen relatif aux données à caractère personnel* : proposition du réseau Trans Europe experts, sous la direction de Nathalie Martial-Braz, Société de Législation comparée, à paraître, p. 192 et s..
- Martial-Braz N., Rochfeld J., Gattone E., « Quel avenir pour la protection des données à caractère personnel en Europe », D. 2013, p. 2788.
- Mattatia F., « CNIL et Tribunaux : concurrence ou complémentarité dans la répression des infractions à la loi informatique et libertés », RSC 2009, p. 317.
- Maxwell W. J, « La jurisprudence américaine en matière de liberté d'expression sur Internet », *in* Conseil d'Etat, *Le numérique et les droit fondamentaux*, Les rapports du Conseil d'Etat, sept. 2014.
- Meuris F., « Que fait la CNIL ? », Comm. Comm. Electr. 2014, alerte 58.
- Molfessis N., « L'exorbitance de l'action de groupe à la française », D. 2014, chron. 947.
- Moulin M.et Younes-Fellous V., « Communication de la CNIL relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données », 2011.
- Osman F., « Avis, directives, codes de bonne conduite, recommandations, déontologie, éthique, etc. : Réflexion sur la dégradation des sources privées du droit », RTDCiv. 1995, p. 528.
- Paiva Melo Marin R., Piolle G. et Bidan C., « An Analysis Grid for Privacy-related Properties of Social Network Systems", *In ASE/IEEE International Conference on Social Computing* (SOCIALCOM 2013), pp. 520--525, Washington D.C., USA, 2013 (IEEE Computer Society, ISBN 978-0-769-5137-1).
- Papin E., « L'application de la loi informatique et libertés du 6 janvier 1978 par les AAI dans le cadre de leurs opérations de saisie », Rev. Lamy dr. immat. mars 2010, n° 58, p. 49.
- Paulik I., « Liberté d'expression par l'image et respect des droits de la personnalité », Petites affiches, 2004, p. 14.
- Pearson S, « Trusted Computing Platforms: TCPA Technology » *in* Context, Prenctice Hall PTR, USA, 2002.
- Pearson S., « Trusted Computing: Strengths, Weaknesses and Further Opportunities for Enhancing Privacy », *In Proceedings of the Third International Conference on Trust Management* (iTrust 2005), Springer Verlag, 2005, 3477, pp. 305-320.
- Pédamon M., « Y a-t-il lieu de distinguer les usages et les coutumes en droit commercial ? », RTD com. 1959, p. 335.

- Perlman R., « The Ephemerizer: Making data disappear », *in Journal of Information System Security* (JISSec), 2005, vol. 1, pp. 51-68.
- Pignatari O., « Droit à l'oubli : la CJUE n'oublie pas les internautes », Revue Lamy Droit de l'Immatériel, 2014, n°107.
- Racine J.-B., « La valeur juridique des codes de conduite privés dans le domaine de l'environnement », RJE 4/1996, p. 413.
- Ravanas J., « Nécessité de trouver le juste équilibre entre la liberté de l'information et le droit de chacun au respect de sa vie privée », JCP G. 2003, II 10085.
- Ravanas J., « Vie privée… », JCP G 1992, II, 21908.
- Ray J.E., « Actualité des TIC », Dr. soc 2013, p978.
- Rebeyrol V., « La nouvelle action de groupe », D. 2014, chron. 940.
- Riché S., Brebner G. et Glitter M., « Client-side profile storage », NETWORKING Workshops on Web Engineering and Peer-to-Peer Computing, 2002, pp. 127-133.
- Roussel B., « Informatisation des dossiers médicaux en milieu hospitalier : intégrité et opposabilité des données numériques », Comm. com. électr. Juin 2009, étude 15.
- Rouvroy A., « Réinventer l'art d'oublier et de se faire oublier dans la société de l'information ? » *in La sécurité de l'individu numérisé, Réflexions prospectives et internationales,* S. Lacour (dir.), L'Harmattan 2010, p.249s..
- Ruet, « L'expression par l'image au regard de l'article 10 de la CEDH », *in Image et droit,* sous la direction de P. Bloch, l'Harmattan 2002.
- Schwyter A. : « Google, oubli moi », JCP G 2014, 1239.
- Shamir A., « How to share a secret », *in Communications of the ACM*, 1979, vol. 22, pp. 612-613.
- Sharma R. and Datta A., "SuperNova: Super-Peers Based Architecture for Decentralized Online Social Networks", *In Fourth international Conference on Communication Systems and Networks* (COMSNETS), pp. 1-10, 2012.
- Starck B., « A propos des accords de Grenelle, Réflexions sur une source informelle du droit », JCP 1970, I, 2363.
- Sweeney L., « k-Anonymity: A Model for Protecting Privacy » *In International Journal of Uncertainty*, Fuzziness and Knowledge-Based Systems, 2002, vol. 10, pp. 557-570.
- Tambou O. : « Les élus locaux et Google : les oubliés du droit à l'oubli », AJ Collectivités Territoriales 2014 p.502.
- Thibierge C., « Le droit souple, Réflexion sur les textures du droit », RTDCiv. 2003, p. 599.
- Thiérache C., « Le droit à l'oubli numérique : un essai qui reste à transformer – Charte du droit à l'oubli dans les sites collaboratifs et les moteurs de recherche du 13 octobre 2010 », Revue Lamy Droit de l'immatériel 2011 – n°67.
- Tilman L., Frimat P., « TIC et santé au travail : la protection des données de santé », JCP éd. S, nov. 2013, 1453.
- Tricoit J-Ph., « Recrutement, rupture du contrat de travail et TIC », JCP S 2013, 1381.

- Trudel P., « Quelles limites à la googleisation des personnes ? » *in La sécurité de l'individu numérisé, Réflexions prospectives et internationales*, S. Lacour (dir.), L'Harmattan 2010, p.47s.
- Turgis S., « La coexistence d'Internet et des médias traditionnels sous l'angle de la Convention européenne des droits de l'homme », RTDH, 2013, n° 93.
- Van Heerde H., Fokkinga M., & Anciaux N., « Balancing privacy and data usability using data degradation » *In Proceedings of the 12th IEEE International Conference on Computational Services and Engineering* (CSE'09), 2009.
- Veilleux A. et Bachand R., « Droit et devoirs des investisseurs : existe-t-il un espace juridique transnational ? » Groupe de recherche sur l'intégration continentale, http://www.unites.uquam.ca/gric.
- Virally M., « Les codes de bonne conduite, pour quoi faire ? » *in, Transfert de technologie, sociétés transnationales et nouvel ordre international,* Ed. J. Touscoz, PUF 1978.
- Walle E. et Savaïdes S., « L'e-réputation sous le prisme du droit du travail », Gaz.Pal 15 octobre 2011, n°288, p.26.
- Wester-Ouisse V., « Le droit pénal face aux codes de bonne conduite », Rev. Sc. Crim. 2000, p. 351s.

LISTE DES ACRONYMES

CEDH: Convention (ou Cour) européenne des droits de l'homme et des libertés fondamentales
CNIL: Commission nationale informatique et libertés
DGCCRF: Direction générale de la concurrence, de la consommation et de la répression des fraudes
DMP: Dossier médical personnel
ENISA : L'Agence Européenne chargée de la sécurité des réseaux et de l'information
EURODAC : système centralisé et automatisé d'identification des empreintes digitales
FING : Fondation Internet nouvelle génération
G29 : Groupe de l'article 29
LCEN : Loi pour la confiance dans l'économie numérique
LIBE (commission): Commission des libertés civiles, de la justice et des affaires intérieures
PNR : Passenger Name Record
RFID : Radio frequency identification
SID : Système d'information douanier
SNIIRAM : Système national informationnel inter-régime d'assurance maladie
SRS: Service de réseautage social
TIC : Technologies de l'information et de la communication
TPM : Trusted Platform Module
VIS : Système d'information des visas

ANNEXE - GUIDE D'ENTRETIEN DROIT A L'OUBLI

1. Le sens général et les représentations sociales

- Si je vous dis, droit à l'oubli, qu'est-ce que cela vous évoque spontanément ?
- Avez-vous déjà eu envie du droit à l'oubli ? Si oui à quelle occasion ?
- Avez-vous déjà communiqué des évènements ou des photos et souhaité les faire disparaître ?
- Idem pour trace numérique et protection de la vie privée ?
- Pour vous personnellement quels seraient les risques liés au numérique ?
- Avez-vous autour de vous déjà entendu parler de mauvaises expériences ? En avez-vous fait vous-même ?
- Avez-vous déjà été sensibilisé aux questions de vie privée et de numérique ? Si oui par qui ? École ? Amis ? Collègues ? Parents ? Médias ? Si oui qui et à quelle occasion ?

2. Les fichiers de données

- Si je vous dis « fichiers de données personnelles » qu'est-ce que cela évoque pour vous ?
- Quels fichiers de données personnelles vous concernant pensez-vous que des tiers détiennent ? Quels tiers ? Quels fichiers ? Connaissez-vous la durée de conservation des données ?
- Quelle serait la bonne durée de conservation des données ?
- Avez-vous déjà vu sur les lieux de ventes physiques ou virtuels des chartes d'usage et des notifications sur la durée de conversation et l'accès aux données personnelles collectées ? Si oui dans quels cas ?
- Avez-vous demandé l'accès à vos données personnelles soit pour les consulter soit pour les modifier ? Si oui à quelle occasion ?
- Avez-vous déjà demandé à un tiers de supprimer un fichier vous concernant ou des données vous concernant ?
- De quels tiers vous méfiez-vous ?
- Ces données peuvent-elles être exploitées ? Vendues ?
- Parmi les données suivantes, lesquelles renseignez-vous sans problèmes ?

	Aucune réticence	Au cas par cas, hésitations	Jamais
Nom et prénom			
Date de naissance ou âge			
Situation maritale			
Adresse postale			
Adresse mail			
Numéro de tél /portable			
Numéro de tel fixe			
Nombre et âge des enfants			
Information sur l'établissement bancaire – quelle banque ?			
Numéro de sécurité sociale			
Profession			
Revenu mensuel			
Orientation religieuse			
Centres d'intérêts			
Orientation sexuelle			
Orientation politique			
Ai-je consommé de la drogue ?			
Ai-je fait de la prison ?			
Ai-je téléchargé illégalement ?			
Autres			

3. Sphère sociabilité amicale – médias sociaux

- Mettez-vous sur la page Facebook de l'enquêté. Que faites-vous avec Facebook ? À quelle fréquence ? Avez qui échangez-vous ? Mettez-vous des photos ? En taguez-vous ?
- Avez-vous des amis que vous ne connaissez pas dans la vie réelle ? si oui comment êtes-vous devenu amis ? Que faites-vous avec eux ?
- Qui met des photos de vous sur Facebook ? Y en-a-t'il que vous souhaitez supprimer ? Avez-vous déjà essayé d'en supprimer ? Cela a-t-il été possible ou non ?
- Avez-vous déjà eu des problèmes de trace numérique ? Si oui quand ? Racontez
- Faites-vous attention à ce que vous postez ou inscrivez sur les murs des autres ?

- Qui écrit sur votre mur ? Avez-vous déjà réduit des autorisations ? Si oui à qui ? Que c'était-il passé pour que vous interdisiez ?
- Avez-vous des anecdotes à raconter à ce sujet pour vous ou des amis ?
- Idem pour les vidéos ….
- Aujourd'hui comment avez-vous paramétré vos options de confidentialité ?
- Avez-vous vu l'évolution des chartes d'usage Facebook ? Avez-vous changé des habitudes et modifié les options de confidentialité ? Si oui expliquez
- Les indications de Facebook sur les options sont-elles claires ?
- Que pensez-vous de la politique de Facebook sur le sujet ?

4. Sphère commerciale

- Sur quels sites achetez-vous sur Internet ? Avez-vous déjà renoncé à des achats pour des questions de confiance ? Payez-vous par carte bancaire en ligne ? Si non comment faites-vous ? Quand avez-vous cessé ?
- Quels sites ou quelles indications ne vous inspirent pas confiance ? Que faut-il pour que vous ayez confiance ?
- Quelles informations avez-vous déjà refusé de donner ? Quelles infos doivent rester privées ?
- Avez-vous déjà regardé ce que les commerçants savent sur vous ? Avez-vous été étonné de toutes les informations qu'ils ont ?
- Sur quels sites êtes-vous enregistré ? Combien de cartes de fidélité avez-vous ?
- Avez-vous hésité ? Modifié vos habitudes ? Si oui pourquoi et à la suite de quoi ?

5. Sphère professionnelle

- Allez-vous sur les sites professionnels tels que Viadeo ou LinkedIn ?
- Si oui, quelles informations refusez-vous de donner ?
- Avez-vous déjà voulu effacer des données personnelles ?
- Avez-vous déjà été étonné de données personnelles mises en ligne par les usagers ?

6. Sphère partage contenu

- Allez-vous sur les sites de partage de contenus tels que Youtube ou Dailymotion ? Si oui, avez-vous déposé des contenus ? À quelle occasion ?
- Avez-vous hésité à en mettre ? Si oui, quelles informations ?

- Avez-vous déjà voulu en effacer ?
- Qu'est-ce qu'Hadopi a changé pour vous ?
- Savez-vous ce que dit le droit français ?
- Qu'est-ce que la e-réputation ?
- Quels conseils donneriez-vous ?
- En conclusion ?

TABLE DES MATIERES